Alma Mater Studiorum · Università di Bologna

**FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI**
**Corso di Laurea Triennale in Informatica per il Management**

# Quantificazione ed individuazione delle alterazioni dei dati nell'ambito di indagini di Informatica Forense

**Tesi di Laurea in Architettura di Internet**

**Relatore:**
**Chiar.mo Prof.**
**MARCO ROCCETTI**

**Presentata da:**
**MARIAGRAZIA CINTI**

**Correlatore:**
**Chiar.mo Prof.**
**CESARE MAIOLI**

**Sessione II**
**Anno Accademico 2010/2011**

*A Riccardo*

# Introduzione

Le legislazioni europea ed italiana non definiscono efficacemente il modo in cui debbano essere trattati i reperti informatici (*hardware*, *software*, metodologie), tuttavia esistono delle best practice, note da diversi anni, che ne descrivono l'opportuno trattamento. Nonostante ciò, errate manipolazioni dei reperti informatici si verificano piuttosto frequentemente a causa della scarsa preparazione della Polizia Giudiziaria operante, dei loro ausiliari e dei consulenti tecnici (si pensi che la legge 48/2008 non prevede oneri per lo Stato, ma questo aspetto verrà trattatato nel paragrafo 3.1.3). Questa cattiva condotta solitamente impedisce che, durante i procedimenti penali, il dato informatico possa diventare prova favorevole o contraria all'indagato stesso. Scopo di questa tesi, e del progetto in essa documentato, è quello di affrontare in modo esaustivo le tematiche tecniche relative alle modalità di trattamento dei dati, utili a fini investigativi e processuali, dimostrando attraverso uno studio sperimentale quanto alcune operazioni maldestre da parte degli operanti possano contaminare ed alterare in maniera irreversibile i dati informatici. Tale studio è stato svolto per definire e quantificare le modificazioni che avvengono su un sistema operativo, quando si eseguono determinate azioni (ideate sotto forma di test). Per rendere tale analisi praticabile e per non avere influenze legate ad altri fattori, si è scelto di ricreare l'ambiente di studio su Virtual Machine e di utilizzare, per ogni singolo test, una nuova ed identica immagine dello stesso ambiente di partenza.

Ma vediamo brevemente il contenuto di ogni capitolo:

Nel capitolo iniziale, verranno introdotti gli elementi fondamentali della *computer forensic*, trattando le motivazioni che hanno condotto alla sua nascita ed alla sua continua evoluzione. Questi importantissimi precetti sono stati successivamente portati dagli Stati Uniti anche agli altri Paesi; in particolar modo verrà fatto riferimento alla situazione italiana ed alla disciplina che qui incarna tali principi: l'informatica forense. Dal punto di vista informatico, verranno definiti i reati e i campi di applicazione in cui è opportuno utilizzare le metodologie forensi, portando ad esempio alcuni casi di cronaca italiana.
Uno dei principali obiettivi dell'informatica forense è garantire l'ammissibilità, in sede processuale, degli elementi acquisiti. Per questo motivo nel secondo capitolo verrà trattata la disciplina alla base dello svolgimento del processo penale. Verranno definiti gli strumenti a disposizione delle parti per rinvenire elementi di carattere informatico ed in particolar modo verrà approfondito il ruolo del consulente tecnico, il suo rapporto con le parti processuali, le sue responsabilità penali.
Nel terzo capitolo ci si occuperà di delineare il panorama giuridico italiano, inquadrando le principali normative legate al contrasto della criminalità informatica ed alla tutela del dato. Nello specifico, verranno trattate le modifiche introdotte al nostro ordinamento dalla Convenzione sul *cybercrime* di Budapest (2001), spiegate le forme di tutela del dato e conseguentemente quelle a tutela del software, delle banche dati e delle altre opere delle ingegno.
Nel quarto capitolo ci si concentrerà sul concetto di dato e sulle sue problematiche metodologiche. Verranno ripercorse tutte le fasi dell'informatica forense e trattate approfonditamente le metodologie da applicare ad ognuna di esse, in riferimento alle linee guida esistenti. Per comprendere il reale funzionamento di ogni operazione tecnica, ne verrano spiegati i concetti informatici alla base, che dovrebbero essere ben conosciuti da qualunque professionista che si trovi a dover trattare il reperto. Successivamente verrà citato un caso di cronaca italiana, Garlasco, in cui la mancanza di criterio nell'esecuzione

di operazioni su uno dei reperti principali ha portato all'inammissibilità di una prova che avrebbe potuto dare esiti ben diversi alla sentenza.
Nel quinto capitolo verranno descritti gli obiettivi e le considerazioni che hanno portato all'esecuzione del progetto collegato a questa tesi. Verranno illustrate le caratteristiche dell'ambiente di studio e riportati i test effettuati, fornendo di volta in volta le opportune chiavi di lettura per la comprensione dei dati prodotti.
Nel capitolo finale verranno mostrati i risultati dello studio, opportunamente analizzati e comparati. Servendosi di alcune rappresentazioni grafiche, verrà analizzato il peso percentuale delle diverse tipologie di operazioni rispetto ad alcuni test specifici e successivamente verranno messi a confronto i test che presentano punti di collegamento.

# Indice

# Elenco delle figure

# Elenco delle tabelle

# Capitolo 1

# L'informatica forense

## 1.1 Le scienze forensi e la prova scientifica

L'uso della prova scientifica per determinare o riscontrare elementi utili all'individuazione dei colpevoli durante un'indagine è una prassi sviluppatasi abbastanza recentemente. I primissimi casi di applicazione del metodo scientifico e della logica possono essere ricondotti alla fine del XVIII secolo quando, per provare la colpevolezza di un'individuo in un caso di omicidio, furono per la prima volta svolti precisi accertamenti tecnici sulla vittima; gli stessi metodi entreranno poi, solo un secolo più tardi, nell'immaginario collettivo grazie ai racconti di *Sir Arthur Conan Doyle* e successivamente di *Georges Simenon* e di *Agatha Christie*.
Con gli anni, l'utilizzo di una qualunque scienza applicata alla risoluzione di questioni di qualche interesse per il sistema legale ha guadagnato l'appellativo di "forense". Il ventaglio delle discipline forensi si è da allora notevolmente ampliato [LZ07]: ad oggi le branche esistenti sono molteplici, si va dalle scienze criminologiche (balistica, analisi delle impronte digitali...), alle scienze sociali (psicologia e psichiatria), alle più recenti scienze forensi digitali (computer forensic, *network forensic*...). Lo scopo ultimo di ognuna di esse è quello di far sì che le prove possano essere validamente utilizzate in sede processuale. Nei paragrafi successivi questo argomento verrà trattato

esaustivamente nei riguardi della computer forensic.

## 1.2 La computer forensic

La computer forensic iniziò a svilupparsi negli Stati Uniti (e in generale anche negli altri Paesi di origine anglosassone) verso la metà degli anni '80, di pari passo con la sempre maggiore accessibilità del grande pubblico ai personal computer e la nascita dei reati ad essi collegati.
Vista la sempre più pressante esigenza di analizzare e raccogliere dati digitali, le forze di polizia iniziarono a mettere a punto tecniche che permettessero di poter validamente utilizzare tali dati in sede processuale, unendo conoscenze giuridiche a specifiche competenze informatiche.
La prima organizzazione investigativa ad istituire un team apposito fu l'FBI che nell'1984 creò il *CART* [1]; questo reparto è ancora oggi attivo ed ha il compito specifico di procedere nei casi in cui si renda necessaria l'analisi di un computer. La successiva tappa che è opportuno ricordare fu la pubblicazione nel 1994 di un insieme di linee guida [ILDti] ad opera del *Dipartimento di Giustizia degli Stati Uniti*, che definirono per la prima volta degli standard sulle modalità operative. Lo svolgersi poi delle prime conferenze internazionali dedicate all'argomento contribuì alla diffusione di questi precetti anche negli altri Paesi.

## 1.3 L'informatica forense in Italia

Con un *gap* di almeno un decennio, anche in Italia iniziò a nascere l'esigenza di reperire, da media digitali, qualunque informazione utile a fini processuali [DD07]. La prima iniziativa a tale riguardo fu l'istituzione nel 1996 del *Nucleo Operativo di Polizia delle Telecomunicazioni*, sviluppatosi parallelamente ad una nuova tipologia di azienda specializzata nel prestare servizi in ambito di sicurezza informatica. Nel 1998 venne infine istituito

[1] Computer Analysis and Response Team.

il *Servizio di Polizia Postale e delle Telecomunicazioni* in cui confluirono le risorse dei dipartimenti precedentemente esistenti.
La disciplina che portò in Italia i precetti della computer forensic è l'informatica forense. Questo termine venne coniato solamente all'inizio degli anni 2000 [2], incarnando la seguente definizione formale [GAM]:

> *"La disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato informatico al fine di essere valutato come prova in un processo, e studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (hard disk, nastri...) nonché l'analisi forense di ogni sistema informatico e telematico (computer, palmare, rete...), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione."*

L'informatica forense comprende dunque tutte le attività rivolte all'analisi e alla soluzione di casi criminali che prevedano, direttamente o meno, l'uso di strumenti informatici. Individuare, acquisire, conservare ed interpretare i dati presenti su un computer sono solo alcuni degli scopi primari di questa disciplina; è necessario che ognuna di queste operazioni venga eseguita utilizzando le migliori tecniche, in modo che venga ridotta al minimo la possibilità di alterazione del supporto informatico, a garanzia che i dati estratti siano identici a quelli originali.
Il divario inizialmente esistente tra Stati Uniti ed Italia si sta gradualmente riassorbendo col passare degli anni, ma ancora si avverte la carenza delle disposizioni italiane su alcuni aspetti. Primo tra tutti la mancanza di un adeguato *know-how* degli operatori, che uniformi le competenze e le metodologie a quelle utilizzate negli altri Paesi. Lodevole è però l'iniziativa di

[2] L'espressione "informatica forense" fu presentata per la prima volta nel 2003 dall'Avv. A. Gammarota durante la presentazione tenuta al I Master CSIG di Bari; le prime lezioni universitarie aventi ad oggetto tale materia si tennero alla Facoltà di Giurisprudenza dell'Università di Bologna a partire dal 2004/2005.

alcuni enti specializzati, che da qualche anno operano per la formazione e specializzazione di periti professionisti: ne è un esempio lo *IACIS* [3].
In Italia la questione della mancanza di un punto di riferimento metodologico è stata sollevata per la prima volta nel 2005, e successivamente nel 2008, durante le sentenze del caso *Vierika* [Im05; Ip08], in cui sono state acquisite in dibattimento proprio le linee guida dello IACIS, ritenute le allora *best practice* delle metodologie d'indagine. In entrambe le occasioni, la difesa dell'imputato si è concentrata sulla correttezza dei metodi di acquisizione, mettendo in discussione l'operato dalla Polizia Giudiziaria. Viene di seguito riportato un passaggio esaustivo della sentenza d'appello:

> *"[...] (procedimento) viziato da ricostruzione tecnico informatica priva di fondamento peritale, ed il correlativo ingiustificato diniego dell'espletamento di perizie, chieste dalla difesa, sulle modalità di generazione e conservazione dei log (registri di collegamento), acquisiti presso il gestore [...], nonché sull'originale del codice sorgente del software per cui è causa."*

Si tratta ad oggi di un argomento molto delicato, per cui andrebbero presi provvedimenti sul piano internazionale, ideando magari delle linee guida ufficialmente riconosciute e attuate dalla maggior parte degli stati.

## 1.4 Reati connessi all'informatica forense

L'eliminazione dei confini tra le persone e le risorse, avvenuta in questi ultimi decenni, ha considerevolmente complicato l'operato delle forze dell'ordine. In una situazione in cui gli illeciti sono sempre più spesso delocalizzati, individuare gli elementi costitutivi di un reato diventa particolarmente complesso; per giungere ad un'appropriata ricostruzione del fatto, ora più che mai deve essere prestata attenzione nella risoluzione dei seguenti quesiti:

[3] The International Association of Computer Investigative Specialists, attivo dal 1990.

- *Da dove?* - dislocazione dell'autore;
- *Quanti autori?* - indeterminatezza degli autori;
- *Chi è? / Chi sono?* - anonimizzazione degli autori;
- *Quando?* - cronologia degli eventi;
- *In che modo?* - modalità esecutive (tenendo conto della volatilità delle tracce e della velocità dell'azione);
- *Perché?* - movente;
- *Quante volte?* - reiterazione;
- *Contro chi?* - offensività.

L'introduzione dell'elemento tecnologico ha avuto ampie ripercussioni anche sulla classificazione dei reati, con l'introduzione di alcune nuove categorie di illecito. Attualmente l'informatica forense si occupa dell'analisi dei dati digitali relativi a:

- **reati informatici e telematici**. Si pensi, ad esempio, a casi di *cracking* o di *phishing*, attività sviluppatesi contestualmente alla diffusione degli elaboratori;
- **reati non informatici ma commessi con sistemi informatici**. Si pensi, ad esempio, al reato di diffamazione a mezzo internet (tramite *blog*, *forum*...);
- **reati di cui si rinvengono tracce o indizi nei sistemi informatici**. Si pensi, ad esempio, al reato di falso in bilancio, di cui si rinvengano tracce delle alterazioni dei dati su i computer della società stessa.

Nel paragrafo 1.5 tale distinzione verrà ulteriormente chiarificata portando ad esempio alcuni casi di cronaca italiana.

Quando ci si trova in uno dei casi sopracitati, è prassi comune partire dall'analisi di tutti i dispositivi rinvenuti sul luogo del reato. Ognuno di essi potrebbe infatti contenere informazioni rilevanti per la risoluzione del caso o fungere da punto di partenza per l'individuazione di nuovi elementi non precedentemente considerati. Non si tratta solamente di ricercare indizi sulla colpevolezza di un individuo, ci si potrebbe anche imbattere in elementi utili a dimostrare il suo alibi, che possano collocare le sue azioni in luoghi ben precisi, descrivere meglio i suoi movimenti e l'ambiente circostante.

## 1.5 Alcuni esempi di cronaca italiana

Facendo riferimento alla classificazione compiuta in precedenza, vengono portati ad esempio alcuni casi di cronaca italiana. Presentiamo, nell'ordine, un esempio di reato informatico, uno di reato commesso tramite sistema informatico e uno di reato di cui si sono rinvenute tracce su sistemi informatici.

### 1.5.1 Caso Vierika

Il "caso *Vierika*" [Im05; Ip08] costituisce un valido esempio di reato informatico nonchè il precursore del suo genere per il sistema giudiziario italiano. Si tratta infatti del primo caso di condanna, emesso nel nostro Paese, nei confronti del creatore di un programma *malware* [4].

#### Ricostruzione dei fatti

L'imputato C.G. è il creatore del malware, da lui stesso denominato "Vereika", che a marzo del 2001 ha iniziato a diffondersi sui sistemi Windows. Questo codice malevolo, scritto in Visual Basic e facente parte della famiglia dei *worm* [5], è stato trasmesso tramite il sito dell'imputato ed è riu-

[4] Si definisce come tale qualsiasi software creato con lo scopo di causare danni più o meno gravi al computer su cui viene eseguito.

[5] Una particolare categoria di malware in grado di autoreplicarsi.

scito in breve tempo ad infettare circa un migliaio di computer. Tale script era composto da due parti collegate: la prima veniva inviata in allagato ad una e-mail e, una volta eseguita, abbassava al minimo le impostazioni di protezione del browser *Internet Explorer*, impostando come home-page dello stesso una determinata pagina del sito dell'indagato; la seconda parte dello script si attivava automaticamente accedendo a tale pagina ed utilizzava gli indirizzi contenuti nel gestore di posta elettronica *Outlook* per replicare l'e-mail iniziale e infettare nuovi computer.

### Esito delle sentenze

Il tribunale di Bologna condannò in primo grado (2005) C.G. per i reati di *"accesso abusivo a sistema informatico o telematico"*(art. 615 ter c.p. nella forma aggravata di cui ai nn. 2 e 3, secondo comma dello stesso articolo) e *"diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"* (art. 615 quinquies c.p.).
La sentenza d'appello (2008) ha riformato in parte la pronuncia del giudice di prima istanza, confermando la sussistenza del reato ma escludendo il verificarsi delle aggravanti.

### Punti salienti

La difesa dell'imputato, nel corso della fase dibattimentale del primo grado di giudizio, mise reiteratamente in discussione la correttezza dei metodi utilizzati dalla Polizia Giudiziaria per quanto concerneva l'estrazione dei dati dal computer dell'imputato e per l'individuazione dello stesso tramite le informazioni detenute da *Tiscali s.p.a.* (provider su cui era registrato il sito dell'imputato) e da *Infostrada s.p.a.* (gestore telefonico dell'imputato).
Come si è convenuto, non era compito del Tribunale quello di definire un giusto protocollo relativo alle procedure informatiche da rispettare in caso di sequestro, ma solo di verificare che i metodi utilizzati dalla Polizia Giudiziaria avessero o meno alterato i dati ricercati. La difesa si limitò solamente a definire tali metodi come non conformi rispetto a quelli previsti dalla (suppo-

sta) migliore pratica scientifica [6], senza però produrre documentazioni relative alle eventuali alterazioni avvenute. Inoltre l'assunzione di paternità del programma, ad opera dall'imputato in sede di interrogatorio, venne utilizzata come giustificazione della non necessarietà di ulteriori approfondimenti tecnici relativi alla questione.

#### L'importanza del dato informatico nella vicenda

I dati informatici utili alla ricostruzione degli eventi sono stati rinvenuti principalmente sul computer dell'imputato (codici sorgenti) e nelle banche dati dei provider di servizi utilizzati dallo stesso. I primi sono stati ottenuti tramite perquisizione e relativo sequestro presso l'abitazione di C.G. e i restanti sono stati forniti liberamente (e forse impropriamente) dai gestori di servizi. Senza di essi non sarebbe stato possibile ricostruire gli eventi né tantomento formulare alcun capo d'imputazione.

### 1.5.2 Vasco Rossi contro Nonciclopedia

Il "caso Vasco Rossi contro Nonciclopedia" costituisce un valido esempio di reato non informatico (diffamazione) commesso su un sistema informatico. Si tratta di una vicenda recentissima ancora in corso di definizione.

#### Ricostruzione dei fatti

Febbraio 2010: l'avvocato del noto rocker italiano Vasco Rossi prende contatto con gli amministratori del sito Nonciclopedia [7] con la richiesta di cancellare la pagina dedicata al rocker, poiché gravemente diffamatoria, e di fornire i dati degli utenti che l'avevano creata per procedere alla loro identificazione. Nonciclopedia risponde di non essere in grado di fornire tali dati, ma che avrebbe provveduto alla rimozione delle parti della pagina ritenute lesive per l'immagine del cantante (come già avvenuto in precedenza per altri

[6] Le linee guida dello IACIS.

[7] Enciclopedia on-line di carattere satirico, attiva dal 2005.

personaggi che avevano ritenuto i contenuti a loro dedicati offensivi), seguendo le indicazioni dello stesso legale. Ad agosto 2011, a più di un anno di distanza e senza avere ricevuto altre comunicazioni, gli amministratori vengono convocati dalla Polizia Postale per avere chiarimenti sul funzionamento del sito. In attesa di ulteriori sviluppi, la pagina viene rimossa. Successivamente nell'ottobre del 2011, come forma di protesta, Nonciclopedia decide di sospendere temporaneamente il servizio [Nonti], per poi riprenderlo qualche giorno dopo.
Da quel momento inizia un tira-e-molla mediatico, che coinvolge da un lato, gli amministratori e i sostenitori di Nonciclopedia che criticano aspramente il comportamente del rocker; dall'altro Vasco stesso che, con continui aggiornamenti di stato (diffusi dal proprio profilo su un *social network*) ritorna più volte sulla sua decisione di querelare gli amministratori del sito, di farne interrompere definitivamente il servizio e di richiedere un adeguato risarcimento per i danni morali subiti. [TPti]

### L'importanza del dato informatico nella vicenda

Il dato informatico in questa vicenda rappresenta un ruolo importantissimo, ossia il mezzo attraverso il quale è avvenuto il presunto reato di diffamazione. Questo illecito (previsto dall'art. 595 c.p.) esiste anche al di fuori dell'ambito informatico, ma in questi ultimi decenni vi ha trovato un validissimo mezzo di diffusione.
Ovviamente il procedimento giudiziario che verrà avviato avrà bisogno di valutare una certa serie di elementi informatici: innanzitutto dovranno essere considerati i log di Nonciclopedia (relativi a contenuti ed autori) detenuti dagli amministratori del sito e dal provider su cui è registrato lo spazio web. Ulteriori elementi potrebbero essere ricercati sui dispositivi in possesso degli amministratori ed eventualmente degli autori della pagina.

### 1.5.3 Omicidio Poggi

Il "caso Garlasco" [pen09], nome con cui è altrimenti nota la vicenda legata all'omicidio di Chiara Poggi, rappresenta un valido esempio di reato di cui si rinvennero tracce su sistemi informatici, nello specifico sul computer del principale indagato: Alberto Stasi.

#### Ricostruzione dei fatti

Il 13 agosto 2007 viene ritrovata morta Chiara Poggi, una ragazza 26enne residente a Garlasco (PV). Secondo una prima ricostruzione, la sera precedente, la vittima ed il fidanzato Alberto Stasi avevano cenato insieme. Stasi ha dichiarato che, dopo cena, ha lasciato la villetta della famiglia Poggi per tornare a casa sua e trascorrervi la notte e, la mattina seguente, ha tentato inutilmente di contattare la Poggi al telefono cellulare. Attorno alle 14 del 13 agosto, il ragazzo si è recato nuovamente presso l'abitazione della Poggi e lì ha trovato la porta aperta: entrato in casa, ha trovato il corpo esanime della ragazza, riverso per terra in un lago di sangue. Lasciata la casa, Stasi si è recato presso la vicina caserma dei Carabinieri per dare l'allarme.
I genitori della ragazza si trovavano fuori città, al momento del delitto.

#### Punti salienti

Il principale indagato Alberto Stasi, ha dichiarato di aver trascorso la mattinata del 13 agosto lavorando alla tesi sul proprio portatile, presso la propria abitazione, provando ripetutamente a contattare la fidanzata sia con il cellulare che con il telefono di casa. L'analisi del telefono cellulare della vittima e dei tabulati dello stesso, ha confermato la serie di chiamate non risposte, così pure l'analisi dei tabulati dell'utenza fissa.
L'analisi del personal computer di Stasi ha invece evidenziato un'impropria gestione dello stesso reperto, ad opera delle forze di polizia a cui era stato affidato, con una serie di ripetuti e scorretti accessi allo stesso. Questo ha reso inutilizzabile, come fonte di prova, il contenuto del computer portatile.

Parallelamente, sul portatile è stato rinvenuto del materiale di carattere pedopornografico, per il quale sono state formulate a Stati delle nuove accuse di detenzione dello stesso. Tale ritrovamento potrebbe inoltre fornire a Stasi un valido movente per l'esecuzione dell'omicidio.

#### L'importanza del dato informatico nella vicenda

L'analisi di tutti i dispositivi rinvenibili sul luogo del reato si dimostra quasi sempre di importanza fondamentale per l'individuazione dei colpevoli, in quanto molto spesso grazie ad essa si riesce a ricostruire l'esatto operato degli indagati, confermando o smentendo eventuali alibi.
I dati informatici presenti sul portatile di Stasi sarebbero stati di enorme importanza nella formazione del giudizio, purtroppo però la loro dimostrata alterazione li ha resi inutilizzabili a tale scopo. Dall'analisi del personal computer si sarebbe potuto verificare o confutare l'alibi fornito dall'indagato, semplicemente controllando le modificazioni intervenute sui file (relativi alla tesi, ma non solo) nel lasso temporale indicato da Stasi. Gli altri elementi analizzati (i telefoni cellulari, l'antifurto di casa Poggi, i tabulati telefonici) si sono invece dimostrati utili allo scopo.

## 1.6 Le cinque fasi dell'informatica forense

Riprendendo la definizione di informatica forense, ossia "l'insieme della tecnica e degli strumenti usati per individuare, acquisire, analizzare, valutare e presentare la prova rinvenuta su un computer o altro dispositivo", possiamo individuare in essa cinque fasi distinte. Analizziamole in dettaglio.

### 1.6.1 Individuazione

La fase di individuazione consiste nella ricerca di qualunque dispositivo che possa contenere dati utili al caso. Si tratta probabilmente della fase di maggior difficoltà di tutta l'indagine, in quanto ogni persona è oggi circon-

data da decine di supporti che possano memorizzare (o celare) informazioni. Non bisogna sottovalutare nessun elemento [GF09], ma anzi considerare le eventuali funzioni secondarie di alcuni dispositivi, ad esempio:

- i lettori multimediali (mp3/mp4) possono essere utilizzati come memorie di massa generiche;
- i drive USB (*mouse*, *hub*, piccoli *gadget* da scrivania...) possono contenere piccole memorie *flash disk*;
- alcune stampanti potrebbero avere un'interfaccia di rete utilizzabile come *repository* di file.

### 1.6.2 Acquisizione e conservazione

La fase di acquisizione consiste nell'ottenere "materialmente" i dati da analizzare. Le forme attravarso cui può essere messa in atto sono la duplicazione o il sequestro.
Solitamente la forma preferita dalle forze dell'ordine è il sequestro, poichè porta con sé vantaggi legati alla semplicità e velocità dell'operazione, le cui uniche attenzioni richieste sono la cura del supporto fisico e un corretto mantenimento della catena di custodia. Inoltre tale procedimento potrebbe consentire di rilevare eventuali evidenze fisiche sul supporto sequestrato (impronte, polveri...) che altrimenti potrebbero venire erroneamente alterate. La procedura alternativa, è la duplicazione del supporto tramite copie bit-a-bit, che può rendersi immediatamente necessaria in sede di perquisizione nel caso in cui i dati risiedano su sistemi inamovibili (perchè di grandi dimensioni o che non possano essere spenti o che non possano privarsi dell'alimentazione elettrica).

I reperti sicuramente più diffusi sono i computer, che molto spesso non vengono gestiti correttamente durante la fase di sequestro, non considerando il

fatto che si tratti di supporti di memorizzazione facilmente alterabili. Nel caso in cui un elaboratore venga rinvenuto acceso è opportuno fare alcune considerazioni prima di procedere oltre. Innanzitutto è fondamentale capire quali dati aspettarsi rispetto al reato che si sta tentando di provare. In alcuni casi potrebbe essere necessario effettuare una copia della memoria RAM, che in quanto volatile con lo spegnimento perderebbe il suo contenuto, per accertare quali programmi fossero in esecuzione in quel preciso momento. Successivamente è necessario scegliere la modalità di spegnimento, tra arresto standard (*shutdown*) e scollegamento dalla rete elettrica (*unplugging*). La prima è solitamente sconsigliabile perchè causa numerose modificazioni ai file di sistema (la natura di queste alterazioni sarà trattata più approfonditamente nei capitoli 4 e 5), ma nei confronti di macchine particolarmente delicate o datate potrebbe rivelarsi fatale per l'hardware, con il rischio di rendere inutilizzabile la macchina.

#### Valutazione specifica di ogni situazione

Anche se il sequestro rappresenta la soluzione più veloce e pratica, non si può stabilire a priori di utilizzare tale metodo, ma è opportuno valutare specificamente ogni situazione. Stesso discorso in relazione alle modalità di spegnimento.

#### Conservazione dei reperti

Dopo l'esecuzione delle operazioni di acquisizione si rende quantomai necessaria una corretta conservazione dei reperti. Nei confronti dei sistemi informatici deve essere prestato un duplice riguardo: occorre considerare la modificabilità della categoria di supporti di memorizzazione a cui appartiene il reperto e successivamente identificare la tecnologia in uso su di esso. In base a tutti questi fattori verrà stabilito il migliore metodo di conservazione dello stesso.

### 1.6.3 Analisi

La fase di analisi deve essere eseguita su una copia del reperto; deve essere riproducibile e ogni singola operazione eseguita deve produrre sempre lo stesso risultato.
All'interno di un computer (o altro dispositivo) potrebbe essere ragionevole ricercare [HOS98]:

- Il contenuto o la data di aggiornamento dei file;
- Dati relativi agli eventi di accensione e spegnimento del sistema;
- L'accesso a specifici documenti o siti (cronologia del *browser*);
- L'orario e il contenuto delle e-mail;
- Conversazioni su sistemi di *Istant Messaging*;
- Elementi che dimostrino la volontà di eliminare o nascondere documenti.

Diversi eventi, non solo quelli sopracitati ma anche altri desumibili da elementi fisici o forensi, possono essere intersecati tra loro per ricostruire la timeline delle azioni di un individuo. Questa importante attività di organizzazione e correlazione dei fatti accumulati prende il nome di *"information management"*.

### 1.6.4 Valutazione

Durante la fase di valutazione viene attribuito un significato ai dati emersi in fase di analisi e ci si accerta della legittimità delle operazioni svolte per acquisirli. [MAI04] Viene emesso un valido giudizio riguardo all'attendibilità, all'integrità e all'autenticità del reperto, valutando attentamente ogni possibile occasione di alterazione dello stesso (chi avrebbe potuto, come e quando).

### 1.6.5 Presentazione

La fase di presentazione dei risultati è il momento in cui il consulente mostra al giudice le prove rinvenute sui reperti e le conclusioni che egli ne ha tratto. Tale presentazione avviene tramite una relazione tecnica che verrà poi presa in esame durante il dibattimento. Il contenuto di tale documento solitamente illustra le metodologie utilizzate e mostra le argomentazioni scientifiche a verifica di tutte le supposizioni. Il suo scopo primario è quello di chiarire a tutte le parti coinvolte nel dibattimento la valenza scientifica e tecnica dei fatti accertati.

# Capitolo 2

# L'elemento informatico nel processo penale

Uno degli obiettivi principali dell'informatica forense è quello di garantire una corretta acquisizione delle prove informatiche, rendendo così possibile l'utilizzazione di tali elementi in sede processuale. Numerosi sono infatti i soggetti, che potrebbero essere interessati all'utilizzo di dati integri e completi al fine di poter valutare ogni fatto giuridicamente rilevante, confermando o confutando ogni supposizione relativa al caso. A ciò deve essere unita una corretta gestione del dato digitale che, come tale, incorpora alcuni problemi metodologici legati alla sua natura complessa: deve essere garantito il rigore tecnico delle procedure utilizzare per il suo trattamento e deve essere tenuto conto della sua natura fisica, che lo rende completamente dipendente dai supporti su cui è conservato.
In questo capitolo ci occuperemo di delineare il panorama giuridico italiano a tale riguardo, inquadrando le principali normative legate alla formazione e all'utilizzo delle prove in ambito informatico. Verranno analizzate le norme che disciplinano lo svolgimento del processo penale, la formazione della prova e l'attuazione degli accertamente tecnici, approfondendo molti degli aspetti riguardanti i consulenti tecnici.
Verrà successivamente data una visione d'insieme alle norme che regolano

i campi d'indagine strettamente connessi all'informatica forense: le forme di contrasto ai crimini informatici o commessi attraverso sistemi informatici, messe in atto a partire dalla ratifica della Convenzione sul cybercrime di Budapest; le normative relative al trattamento dei dati personali, anche ad opera dei soggetti coinvolti nel processo e infine la disciplina del diritto d'autore che tutela le opere dell'ingegno, i software e le banche dati.

## 2.1 Lo svolgimento del processo

L'articolo 111 della Costituzione disciplina lo svolgimento del processo penale, definendo alcune disposizioni atte a garantire un giusto processo.

> *La giurisdizione si attua mediante il giusto processo regolato dalla legge. Ogni processo si svolge nel contraddittorio tra le parti, in condizioni di parità, davanti al giudice terzo e imparziale. La legge assicura che la persona accusata del reato disponga del tempo e delle condizioni necessari per preparare la sua difesa; di ottenere l'acquisizione di ogni altro mezzo di prova a suo favore. Il processo è regolato dal principio del contraddittorio nella formazione della prova. La legge regola i casi in cui la formazione della prova non ha luogo in contraddittorio per consenso dell'imputato o per accertata impossibilità di natura oggettiva.*

É opportuno focalizzare l'attenzione su alcuni punti dell'articolo citato:

- La prova si forma in dibattimento, ossia durante la dialettica tra le parti, nei confronti di una delle quali potrà essere fatta valere;
- La persona accusata del reato, che deve essere informata nel più breve tempo possibile riguardo alle accuse a suo carico, dispone del tempo e delle condizioni necessarie per preparare la sua difesa. Ciò vuol dire che ha le facoltà di far interrogare le persone che possano rendere dichiarazioni a suo carico e di ottenere l'acquisizione di ogni altro mezzo di prova a suo favore;

- La legge regola i casi in cui la formazione della prova non ha luogo in dibattimento, ossia gli atti di indagine a prevedibile irripetibilità sopravvenuta. É questo il caso degli accertamenti tecnici non ripetibili [Si veda il paragrafo 2.5].

## 2.2 Definizione di prova

Il Codice di procedura penale disciplina in modo esaustivo i fatti che possono divenire oggetto di prova, [1] ma non lo fa in maniera tassativa: lascia infatti al giudice la possibilità di ammettere in giudizio qualunque prova, purchè essa risulti idonea a risalire alla verità dei fatti e non leda la libertà morale della persona. [2]

## 2.3 La perizia

La perizia è uno dei *mezzi di prova*, ossia uno degli strumenti direttamente utilizzabili dal giudice in sede processuale. É disciplinata dal Codice di procedura penale [3] ed è ammessa quando occorre svolgere indagini oppure acquisire dati o valutazioni che richiedano specifiche competenze tecniche, scientifiche o artistiche. Può essere disposta d'ufficio dal giudice con ordinanza motivata; in questo caso il giudice dispone la nomina del perito e definisce tutti gli opportuni provvedimenti che sono necessari per il suo corretto svolgimento. [4] Una volta disposta la perizia, entrambe le parti processuali hanno la possibilità di nominare i propri consulenti tecnici, in numero non superiore a quello dei periti. [5]
Tuttavia, anche quando non è disposta la perizia, ciascuna parte può nomi-

[1] art.187 c.p.p.
[2] art.189 c.p.p.
[3] art.220 c.p.p.
[4] art.224 c.c.p.
[5] art.225 c.p.p.

nare, in numero non superiore a due, i propri consulenti tecnici con lo scopo di ricercare elementi a favore delle supposizioni della parte.

## 2.4 Mezzi di ricerca della prova

Il Codice di procedura penale disciplina anche i *mezzi di ricerca della prova*, ossia gli strumenti di indagine che consentano di acquisirla. Facendo particolare riferimento al dato informatico, tali disposizioni si rivolgono direttamente alla Polizia Giudiziaria ed ai difensori delle parti, e riguardano le ispezioni, le perquisizioni, i sequestri probatori e le intercettazioni; vediamo più dettagliatamente questi strumenti perchè di fatto rappresentano il mezzo attraverso il quale possono essere messe in atto le operazioni di informatica forense.

### 2.4.1 Ispezioni

L'ispezione [6] consiste in un accertamento che può avere ad oggetto persone, luoghi o cose; tale accertamento tende a limitare talune libertà costituzionali (libertà personale, libertà domiciliare...) per cui la legge prevede delle garanzie sostanziali al fine di limitare il meno possibile tali libertà. La creazione di una copia conforme al reperto può essere eseguita in questa sede utilizzando le apposite strumentazioni (hardware e software) [Si veda il paragrafo 4.1.1].

### 2.4.2 Perquisizioni

La perquisizione [7] è un'attività diretta ad individuare e acquisire il corpo del reato o cose ad esso pertinenti, ovvero ad eseguire l'arresto dell'imputato o dell'evaso; tale accertamento, come l'ispezione, tende a limitare talune libertà costituzionali (libertà personale, libertà domiciliare...) per cui la

[6] art.244 e segg. c.c.p.
[7] art.247 e 253 c.c.p.

legge prevede delle garanzie sostanziali al fine di limitare il meno possibile tali libertà. La creazione di una copia conforme al reperto può essere eseguita in questa sede utilizzando le apposite strumentazioni (hardware e software) [Si veda il paragrafo 4.1.1].

### 2.4.3 Sequestri Probatori

Il sequestro probatorio è strettamente collegato alla perquisizione, essendone spesso una diretta conseguenza. L'Autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose ad esso pertinenti necessarie per l'accertamento dei fatti. [8] Laddove non sia possibile l'intervento tempestivo dell'Autorità giudiziaria è consentito agli ufficiali di Polizia Giudiziaria sequestrare gli stessi beni prima che si disperdano. In particolare il codice disciplina il sequestro di corrispondenza, [9] titoli, valori, e somme in conti correnti. [10]

### 2.4.4 Intercettazioni

L'intercettazione [11] è un'attività diretta a captare comunicazioni e conversazioni, nonché flussi di comunicazioni informatiche o telematiche. Anche questo strumento tende a limitare alcune libertà costituzionali, fra cui la libertà di comunicazione del pensiero e la libertà domiciliare, per cui sono previste particolari norme procedurali volte a garantire la legittimità formale e sostanziale dell'attività.
Le tecniche a disposizione delle forze di polizia sono diverse, ma la più utilizzata in termini numerici è l'*intercettazione telefonica* richiesta agli operatori telefonici, che sono obbligati ad adempiere utilizzando le proprie strutture tecnologiche ed organizzative. Vi sono poi le *intercettazioni ambientali*, realizzate principalmente con l'impiego di microspie e telecamere nascoste,

[8] art.253 c.p.p.
[9] art. 254 c.p.p.
[10] art. 255 c.p.p.
[11] art.266 e segg. c.p.p.

e le *intercettazioni informatiche* attuate con specifici strumenti hardware e software.

## 2.5 Disciplina dell'accertamento tecnico

L'accertamento tecnico è uno strumento che si rende necessario quando, per l'analisi di una determinata situazione, occorrono specifiche competenze. Queste saranno esercitate dal consulente tecnico incaricato, tramite accertamenti, rilievi segnaletici, fotografici o descrittivi. Tali elementi riscontrati, se ammessi dalla corte, diventeranno mezzi di prova.

### 2.5.1 Accertamento tecnico ripetibile

Anche se il termine *accertamento tecnico ripetibile* non è contenuto nel Codice di proceduta penale, in tale definizione possono essere fatti rietrare tutti accertamenti svolti dai consulenti tecnici, esclusi quelli previsti dall'art.360 c.p.p. (accertamenti tecnici non ripetibili).

### 2.5.2 Accertamento tecnico non ripetibile

L'accertamento tecnico non ripetibile [12] riguarda persone, cose o luoghi il cui stato è soggetto a modificazione. Dato che un'indagine tecnico-scientifica rischia di compromettere l'integrità delle prove, viene concordato tra le parti il momento del suo effettivo svolgimento. É il Pubblico Ministero a prendere l'iniziativa, avvisando la persona sottoposta alle indagini, la persona offesa dal reato e i difensori riguardo al giorno, all'ora e al luogo fissati per il conferimento dell'incarico; deve inoltre comunicare loro la facoltà di nominare consulenti tecnici. I difensori nonché i consulenti tecnici eventualmente nominati, hanno diritto di partecipare agli accertamenti e di formulare osservazioni o riserve. Tali disposizioni si applicano anche nei casi in cui l'accertamento

[12] art.360 c.p.p.

tecnico determina modificazioni delle cose, dei luoghi o delle persone, tali da rendere l'atto *non ripetibile*. [13]

## 2.6 Consulenti tecnici

### 2.6.1 Consulenti tecnici d'ufficio

Il consulente tecnico d'ufficio (o CTU) lavora come ausiliario del giudice operando per lo stesso in un rapporto di stretta fiducia e nel rispetto delle rigide e precise competenze delineate dal Codice di procedura civile.
Solitamente il consulente tecnico è scelto tra le persone iscritte all'apposito *Albo di categoria detenuto dal Tribunale* (il professionista è obbligato ad assumere tale incarico [14]), ma dato che tale rapporto deve essere strettamente fiduciario, il giudice ha la facoltà di poter nominare anche esperti non iscritti a tale Albo (ma in questo caso non vi sono obblighi per il professionista).
Lo scopo a cui è principalmente preposto il consulente tecnico d'ufficio è quello di rispondere in maniera puntuale e precisa ai quesiti che il Giudice formula nell'udienza di conferimento dell'incarico e di esporne i risultati in un'apposita relazione che prende il nome di *Consulenza Tecnica d'Ufficio*.
In particolare [AM06] è importante che il consulente faccia sempre riferimento a dati certi e, possibilmente, che accompagni tutto ciò che afferma con opportuna documentazione. Le conclusioni che espone al termine della propria relazione devono essere il risultato di un procedimento logico ben preciso, ma non devono contenere in alcun modo giudizi che possano influenzare le decisioni del giudice. Inoltre deve prestare particolare attenzione nel garantire la propria imparzialità nei confronti delle parti alle quali deve consentire, in ogni momento, il contradditorio.

[13] art.117 delle norme di attuazione
[14] art. 63 c.p.p.

### 2.6.2 Consulenti tecnici di parte

Il consulente tecnico di parte (o CTP) è uno strumento autonomo, alternativo alla perizia, al quale ciascuna delle parti può ricorrere. É solitamente un professionista del campo tecnico-scientifico, al quale è stato conferito l'incarico di accertare determinati aspetti legati ad uno specifico settore e di svolgere le proprie osservazioni a supporto della parte che lo ha nominato.
Il Pubblico Ministero ha l'obbligo di scegliere il proprio consulente tecnico dall'Albo detenuto presso il tribunale, invece il difensore ha una più ampia libertà di scelta in merito alla natura fiduciaria del rapporto tra professionista e parte.
Il consulente di parte assume un ruolo fondamentale per la risoluzione di questioni che, sempre più spesso, dipendono da valutazioni di carattere tecnico molto precise, operando all'interno di un rapporto professionale completamente disciplinato dal diritto privato. Il consulente tecnico di parte, infatti, è sempre pagato dalla parte che lo nomina (la quale potrà al massimo, in caso di vittoria, recuperare le spese di causa) ed ha diritto di essere compensato in relazione alla propria parcella professionale o in base ad eventuali accordi stipulati con il cliente.
Al contrario del consulente tecnico nominato dal giudice, il perito di parte è esonerato da qualsiasi obbligo di cooperazione nei confronti dell'autorità giudiziaria, al di fuori del divieto di ostacolare illegittimamente l'attività del consulente del giudice. Dovrebbe comunque rispettare i principi stabiliti dal proprio codice deontologico (se presente) e dai tradizionali parametri di correttezza professionale, legalità e moralità.

### 2.6.3 Responsabilità penali dei periti e consulenti

I consulenti tecnici e i periti hanno delle specifiche responsabilità penali nello svolgimento delle operazioni a cui sono preposti. I reati a cui potrebbero incorrere con le loro azioni sono:

- **Falsa perizia o interpretazione** [15] nel caso in cui il perito dia pareri o interpretazioni mendaci, affermando fatti non conformi al vero. La pena prevista è la reclusione da due a sei anni, oltre all'interdizione dai pubblici uffici e dalla professione.

- **Frode processuale** [16] è l'atto commesso da chiunque nel corso di un procedimento civile o amministrativo, immuti artificiosamente lo stato dei luoghi o delle cose o delle persone, al fine di trarre in inganno il giudice. É punito, qualora il fatto non sia preveduto come reato da una particolare disposizione di legge, con la reclusione da sei mesi a tre anni.

- **False dichiarazioni o attestazioni in atti destinati all'autorità giudiziaria**, [17] salvo che il fatto costituisca più grave reato, sono punite con la reclusione da uno a cinque anni.

- **Intralcio alla giustizia (subordinazione)** [18] secondo cui, chiunque offra o prometta denaro o altra utilità alla persona chiamata a rendere dichiarazioni davanti all'autorità giudiziaria ovvero a svolgere attività di perito, consulente tecnico o interprete, per indurla a commettere i reati previsti dagli articoli 371 bis, 372 e 373, soggiace alle pene previste dagli stessi articoli, ridotte dalla metà ai due terzi e all'interdizione dai pubblici uffici.

[15] art.373 c.p.
[16] art.374 c.p.
[17] art.374bis c.p.
[18] art.377 c.p.

# Capitolo 3

# Il panorama normativo italiano

## 3.1 Convenzione sul cybercrime di Budapest e sua ratifica

La *Convenzione sul cybercrime di Budapest* del 2001, ratificata in Italia dalla *Legge n.48 del 18 marzo 2008*, è probabilmente il testo normativo più rilevante in ambito di computer forensic. Questo importante trattato, che rappresenta il primo accordo internazionale relativo alle forme di contrasto dei crimini informatici o commessi attraverso sistemi informatici, ha modificato il panorama normativo italiano, già particolarmente competente in materia di reati informatici dal punto di vista normativo, ma non sufficientemente da quello tecnico.
Tale convenzione è stata redatta con lo scopo di realizzare una politica europea comune in grado di coordinare e rendere più efficace la lotta ai crimini informatici. In particolare, ha voluto uniformare il concetto di reato legato alla criminalità informatica, dotando i Paesi firmatari di strumenti adeguati allo svolgimento delle indagini e al perseguimento dei crimini correlati all'area informatica. Ha costituito infine un efficace regime di cooperazione internazionale che miri ad essere il più ampio possibile, che si estenda a tutti i reati relativi a sistemi e a dati informatizzati e che sia conforme agli accordi internazionali in materia.

### 3.1.1 Modifiche al Codice Penale

La Legge di ratifica 48/2008 ha portato alle seguenti modifiche degli articoli del codice penale:

**Art.491 bis (documenti informatici)**

> *Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato,* ***avente efficacia probatoria****, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.*
> RIMOSSO: **A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.**

**Art.244 (casi e forme delle ispezioni)**

> *1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.*
> *2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autority giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autority giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica* ***anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione****.*

**Art.247 (casi e forme delle perquisizioni)**

*1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.*

*1.bis* ***Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione****.*

*2. La perquisizione è disposta con decreto motivato.*

*3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.*

**Art.248 (richiesta di consegna)**

*1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.*

*2. Per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare* ***presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici****. In caso di rifiuto, l'autorità giudiziaria procede a perquisizione.*

**Art.254 (sequestro di corrispondenza telematica)**

SOSTITUITO: *1.* ***Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa o che comunque possono avere relazione con il reato.***

*2. Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli* ***o alterarli*** *e senza prendere altrimenti conoscenza del loro contenuto.*

*3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.*

**Art.254bis (sequestro di dati informatici di traffico)**

*1.* ***L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.***

**Art.256 (dovere di esibizione)**

*1. Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato,* ***nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto****, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione.*

*2. Quando la dichiarazione concerne un segreto di ufficio o professionale, l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro.*

*3. Quando la dichiarazione concerne un segreto di Stato, l'autorità giudiziaria ne informa il Presidente del Consiglio dei Ministri, chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato.*

*4. Qualora, entro sessanta giorni dalla notificazione della richiesta, il Presidente del Consiglio dei Ministri non dia conferma del segreto, l'autorità giudiziaria dispone il sequestro.*

**Art.259 (custodia delle cose sequestrate)**

*1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode,*

*idoneo a norma dell'articolo 120.*

*2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia.* ***Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria.*** *Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.*

**Art.260 (sigillo elettronico o informatico e copia dei dati)**

*1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo,* ***anche di carattere elettronico o informatico****, idoneo a indicare il vincolo imposto a fini di giustizia.*

*2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'articolo 259.* ***Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o***

***dalla segreteria.***

*3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione.*

**Art.352 (perquisizioni)**

*1. Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.*

*1-bis.* ***Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.***

*2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata per uno dei delitti previsti dall'articolo 380 ovvero al fermo di una persona indiziata di delitto, gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo de-*

*creto di perquisizione.*

*3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'articolo 251 quando il ritardo potrebbe pregiudicarne l'esito.*

*4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.*

**Art.353 (corrispondenza telematica)**

*1. Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.*

*2. Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata e* ***l'accertamento del contenuto****.*

*3. Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza,* ***anche se in forma elettronica o se inoltrati per via telematica****, per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale,* ***telegrafico, telematico o di telecomunicazione*** *di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati.*

**Art.354 (accertamenti urgenti e sequestro)**

*1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.*

*2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose.* ***In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità****. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.*

*3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.*

### 3.1.2 Modifiche al Codice della Privacy

La Legge di ratifica 48/2008 ha introdotto i seguenti commi all'articolo 10 del Codice della Privacy:

**Art.10 (conservazione dei dati di traffico)**

*4-ter. Il Ministro dell'interno o, su delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n.271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n.271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.*
*4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conse-*

*guentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. 4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.*

### 3.1.3 Considerazioni riguardo all'attuazione

La legge di ratifica è entrata in vigore il giorno dopo essere stata pubblicata sulla Gazzetta Ufficiale. [1] La relazione accompagnatoria [2] utilizzò le seguenti parole per definirla:

*[...] Dal provvedimento in esame non derivano nuovi o maggiori oneri a carico del bilancio dello Stato [...]*

ma onestamente è molto difficile considerare tale legge *a costo zero*, poichè i costi legati all'hardware, al software, allo humanware ed alla logistica a fronte dell'adeguamento a tali disposizioni sono stati elevati.
Nella stessa relazione, la ratifica viene definita come:

*[...] un adeguamento prevalentemente lessicale delle disposizioni processuali già vigenti [...]*

ma anche qui occorre aprire una parentesi. Infatti non è del tutto vero, in quanto il legislatore italiano sostituì il termine originale *data*, con parole dai significati ben diversi come ad esempio *dati*, *informazioni* e *programmi*, che ebbero importanti ripercussioni sull'ambito di applicazione delle diverse norme.

[1] Gazzetta Ufficiale n.40 del 4 aprile 2008.
[2] Al disegno di legge n. 2807 del 19 giugno 2007.

Infine la scelta di eccepire tali disposizioni all'interno del Codice Penale, e non ad esempio in un codice specifico, portò ad un'inattesa estensione del campo di applicabilità delle disposizioni definite dalla convenzione, nonché ad alcune imprecisioni. A tal riguardo si può ad esempio citare il testo dell'articolo 353, terzo comma, che si riferisce testualmente a

> *Pieghi, pacchi [...] anche se in forma elettronica o se inoltrati per via telematica.*

## 3.2 Normativa sul trattamento dei dati personali

### 3.2.1 Testo unico sulla privacy

I dati personali sono tutelati principalmente dal *Decreto Legislativo 196/03* intitolato *Codice in materia di protezione dei dati personali*, noto anche come *Codice della privacy* o *Testo unico sulla privacy*. Sulla corretta applicazione delle norme in esso contenuto vigila l'*Autorità Garante per la protezione dei dati personali*.
Il suo scopo primario è quello di riconoscere il diritto del singolo sui propri dati personali e, conseguentemente di disciplinare le diverse operazioni di gestione (definite trattamento) dei dati, come la raccolta, l'elaborazione, la modificazione, o la diffusione degli stessi.

### 3.2.2 Delibere del Garante della privacy

Il Garante per la protezione dei dati personali è un'autorità amministrativa istituita per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali. I suoi compiti sono molteplici, ma principalmente si occupa del controllo della correttezza del trattamento dei dati e dell'esame dei reclami e delle segnalazioni ricevute.

Molte sono le delibere emesse dal Garante di qualche interesse per i soggetti connessi all'informatica forense, tra le quali ricordiamo:

- **Del.Garante 46/08**, Trattamento dei dati ad opera dei consulenti tecnici e periti del giudice e del Pubblico Ministero;
- **Del.Garante 178/08**, Recepimento normativo su traffico telefonico e telematico;
- **Del.Garante 60/08**, Trattamento dei dati nell'ambito dello svolgimento di investigazioni difensive;
- **Del.Garante 35/08**, Trattamento dei dati ad opera dei liberi professionisti;
- **Del.Garante 37/08**, Trattamento dei dati ad opera degli investigatori privati.

## 3.3 Normativa sul diritto d'autore

Il diritto d'autore è una posizione giuridica che trae le sue origini già dal lontano 1400, momento in cui, in particolar modo a Venezia, iniziò a nascere la necessità degli stampatori e copisti di poter copiare determinate opere. Inizialmente tale diritto era conferito dal Doge per rispondere alla specifica richiesta del controllo dei contenuti, nascendo così come diritto di un terzo e non dell'autore stesso dell'opera. Inizia a consolidarsi intorno al 1600, ma solamente nel 1800 trova spazio nel Codice Civile Napoleonico, in cui nascono i concetti di *autore* e di *diritto morale*. [3] Da quel momento anche in Italia iniziano a svilupparsi normative specifiche che diventarono nazionali con l'Unità d'Italia. Attualmente la tutela del diritto d'autore è disciplinata dalla *Legge 633/1941*.

[3] É un diritto della personalità, e come tale è intrasmissibile, inalienabile e imprescrittibile. Nasce nel momento in cui l'opera viene creata, senza la necessità di alcuna registrazione.

### 3.3.1 Legge 633/1941

Le opere tutelate dal diritto d'autore sono le seguenti:

- **Opere dell'ingegno** di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione;

- **Programmi per elaboratore**, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso;

- **Banche di dati** intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto;

I diritti che sono riconosciuti agli autori delle opere sono principalmente:

- **Diritti morali**, mirano a tutelare la personalità dell'autore, il suo onore e la sua reputazione. Sono per loro natura imprescrittibili, irrinunciabili, inalienabili e autonomi (ossia indipendenti dai diritti di sfruttamento economico). Rendono disponibili all'autore una serie di facoltà, quali: il diritto alla paternità dell'opera, il diritto all'integrità dell'opera, il diritto di pentimento e il diritto d'inedito.
  Estinto il diritto d'autore, l'opera diviene di pubblico dominio ed è liberamente utilizzabile da chiunque, anche a fini economici, purché sia rispettato il diritto morale alla titolarità artistica.

- **Diritti di utilizzazione economica**, ossia i diritti patrimoniali che derivano dall'utilizzo economico dell'opera, in ogni forma e modo. Sono

raggruppabili in tre categorie principali: diritti di riproduzione e distribuzione, diritti di comunicazione al pubblico e diritti di traduzione ed elaborazione. Questi diritti durano tutta la vita dell'autore e fino a 70 anni dopo la morte di quest'ultimo.

# Capitolo 4

# Trattamento di reperti informatici tra teoria e pratica

Alla luce di quanto esposto dalle normative vigenti, e approfittando dei concetti definiti come ottimali dalle linee guida sull'argomento, è possibile delineare il corretto comportamento di chiunque debba approcciarsi ad un reperto informatico. Analizziamo tali metodologie, partendo dal *workflow* rappresentato alla Figura 4.1.

## 4.1 Acquisizione: come procedere

La fase di acquisizione, già ampiamente trattata nel paragrafo 1.6.3, è fondamentale per il buon fine delle successive operazioni e per l'ammissione a giudizio degli elementi riscontrati sul reperto. Questa è sicuramente la fase più delicata, in cui il minimo errore potrebbe portare a gravi contaminazioni [MG02]. Anche per questo motivo è indispensabile produrre un'opportuna documentazione di tutte le operazioni svolte, spiegando i fattori che hanno spinto ad assumere determinate decisioni.
Il *computer forenser*, chiamato ad intervenire in uno specifico caso, deve valutare attentamente tutti gli elementi che lo circondano, prima di poter

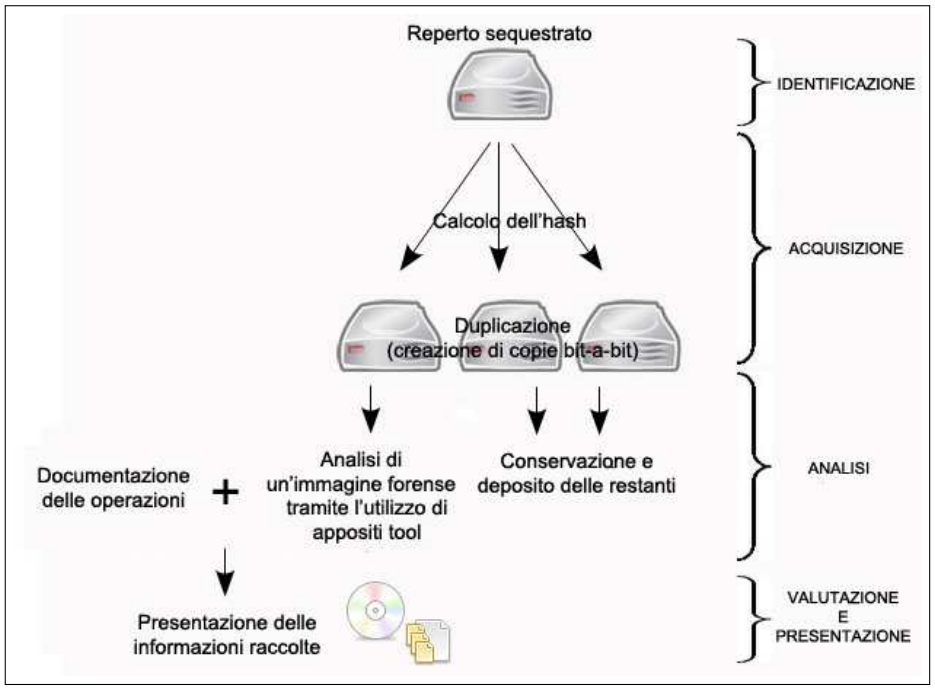



Figura 4.1: Schematizzazione fasi e best practice.

procedere. Innanzitutto vi sono due situazioni ben distinte in cui potrebbe trovarsi: rinvenimento di un dispositivo acceso o di uno spento.

### Nei confronti di un dispositivo acceso

Se il forenser si trova davanti ad un dispositivo acceso deve valutare (anche in merito al reato che sta cercando di provare) se è opportuno effettuare una copia della memoria RAM per ottenere informazioni riguardanti l'uso che si stava facendo della macchina, potendo facilmente determinare le funzionalità dei software ivi in esecuzione.
Sarebbe opportuno, prima di spegnere la macchina, verificare se sulla stessa siano attivi programmi di cifratura dei dati, che potrebbero rendere l'intero contenuto del dispositivo inutilizzabile senza l'opportuna *passphrase*, che molto probabilmente sarebbe impossibile da reperire successivamente.

Nel determinare la modalità di spegnimento della macchina, è opportuno tenere conto dello stato dell'hardware. Sistemi particolarmente delicati infatti potrebbero non essere in grado di sostenere le conseguenze di uno scollegamento dalla rete elettrica (unplugging); benché questa sia la tecnica preferibile perchè non genera modificazioni nei file di sistema, in alcune situazioni sarebbe assolutamente da preferirsi lo shutdown.

#### Nei confronti di un dispositivo spento

Genericamente non si riscontrano particolari problemi nell'approcciarsi ad una macchina spenta e si può passare quasi immediatamente al sequestro. Prima di sigillare il dispositivo sarebbe però opportuno verificare almeno teoricamente il suo funzionamento (magari controllando l'hardware), per evitare di incorrere successivamente in spiacevoli inconvenienti. Ad esempio si dovrebbe verificare la presenza di eventuali dischi cifrati e di dischi RAID.
Molti altri sono i fattori che andrebbero tenuti in considerazione; nelle righe precedenti ci si è limitati a descrivere un paio di situazioni possibili, che non sono assolutamente da ritenersi le uniche.

### 4.1.1 Creazione di bit-stream image

Uno dei principi fondamentali su cui si basa lo svolgimento degli accertamenti tecnici ripetibili, è il fatto che le procedure operate in questa fase debbano essere controllabili e ripetibili. Per questo motivo ogni azione atta ad individuare od estrarre dati da un dispositivo non può essere eseguita sul supporto originale, ma su una sua copia forense dello stesso, detta copia bit-a-bit (o *bit stream image*).
Ci sono poche ma ragionevoli accoratezze da rispettare per non alterare il supporto che si vorrebbe acquisire. Innanzitutto, è opportuno impostare un blocco in scrittura al sistema, al fine di non comprometterne l'integrità. Ciò è facilmente praticabile ricorrendo ad apposite apparecchiature hardware (*write block*, di cui è mostrato un esempio alla Figura 4.2), oppure a specifiche


Figura 4.2: Uno strumento indispensabile: il write block.

soluzioni software. [1] Quando vi è la necessità di utilizzare un sistema Windows, si dovrebbero sempre ricorrere a strumenti per il blocco della scrittura, oppure a tool forensi specifici [Paragrafo 4.2.2]. É necessario utilizzare dischi di destinazione vergini, e ricorrere sempre ad hardware o software dedicati alla copia. Sempre più spesso le suite forensi uniscono in un unico prodotto strumenti utili alla fase di acquisizione e a quella di analisi.

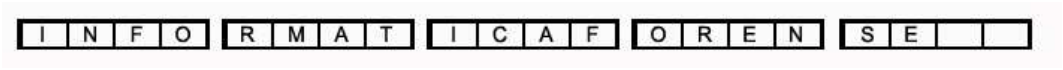
Per duplicare i dati contenuti in un dispositivo si ricorre all'utilizzo di copie bit-a-bit perchè sono l'unico modo di rispettare l'interezza del reperto. In esso infatti non esistono solamente i dati in quanto tali, ma tutta una serie di informazioni che possono essere raccolte intorno ad essi. Il contenuto di un hard disk ad esempio non è composto solamente da spazio allocato, ma comprende anche quello non allocato e gli *slack space*, che possono fornire altrettanto utili informazioni. Per comprendere meglio questi concetti, è opportuno aprire una parentesi sul funzionamento del file system di un computer.

[1] Tale opzione è praticabile solamente su sistemi Unix.

### Slack space, spazio allocato e non allocato

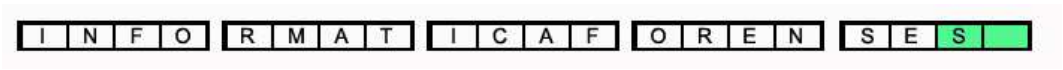
All'interno di ogni sistema opera il file system, uno strumento che si occupa di gestire la memorizzazione dei file sull'hard disk; quando accediamo ad un file ("doppio click"), non facciamo altro che chiedere al sistema operativo di recuperare tali informazioni e di mostrarcele. Generalmente i file, sono suddivisi in parti e scritti all'interno dei blocchi che compongono la memoria nel dispositivo; questi blocchi sono di dimensione fissa e per questo spesso non vengono riempiti completamente.

Portiamo ad esempio una situazione estremamente semplificata: supponiamo di dover memorizzare la stringa "Informatica Forense" [Figura 4.3, caso a] in blocchi da quattro caratteri ciascuno. Così facendo, occupiamo 18 caratteri sui 20 che sono a disposizione, lasciando due spazi inutilizzati, apparentemente vuoti (e che non possono essere riempiti da altre stringhe perchè il blocco è già assegnato). Questi blocchi in precedenza potevano essere allocati in altra maniera. Immaginiamo che vi fosse memorizzata la stringa "la computer forensics" [Figura 4.3, caso b], che ne occupava 19 caratteri su 20, e che successivamente questa sia stata cancellata. La nuova stringa avrebbe sovrascritto i caratteri precedenti [Figura 4.3, caso c], lasciando inutilizzati il 19° e il 20° spazio, che conserverebbero porzioni residue dei vecchi dati:




(a) Stringa "informatica forense" memorizzata in blocchi da 4 caratteri ciascuno


(b) Situazione precedente: stringa "la computer forensic" memorizzata negli stessi blocchi




(c) Situazione reale, lo slack space (evidenziato) contiene dati residui

Figura 4.3: Rappresentazione del concetto di slack space.

queste informazioni (evidenziate in figura) prendono il nome di slack space. Tutti questi elementi di basso livello, possono essere molto utili per risalire a file o a parti di essi (anche volutamente) cancellati: l'analisi completa di un hard disk deve prevedere necessariamente anche la loro comprensione.
Creare una copia bit-a-bit di un supporto è l'unico modo per preservare tali informazioni e per non alterare i metadati dei file ancora esistenti; il banale copia-incolla o il *drag-and-drop* degli stessi ne modificherebbe, ad esempio, la data di creazione e di ultimo accesso. Inoltre la creazione di più copie ha una certa praticità, permettendo di suddividere il lavoro tra più persone.

### 4.1.2 Apposizione di un sigillo (informatico)

Avendo a disposizione il reperto sequestrato, appare evidente la necessità di apporre ad esso un sigillo, in modo da poter riscontrare eventuali successive alterazioni derivanti da un improprio utilizzo dello stesso reperto. Non stiamo però parlando di un sigillo materiale, ma di uno informatico: l'utilizzo di una funzione *hash* sul contenuto del reperto genera un valore hash (anche detto *digest* o *fingerprint*) che identifica quasi univocamente l'insieme dei dati su cui è stato calcolato. Approfondiamone il funzionamento.

#### Funzione hash

Una funzione hash è una funzione che, dato un valore iniziale x, genera un valore hash y che appartiene ad un dominio molto diverso da quello del valore di partenza.

$$f : x \longrightarrow y \qquad \forall\ |x| = n,\ |y| = m \qquad t.c. \quad n \gg m$$

Al nostro scopo occorre però una funzione, detta *hash one-way*, con determinate caratteristiche:

- Deve essere facile da calcolare;
- Deve essere (computazionalmente) complessa da invertire;

- Deve essere complesso trovare un altro valore x che generi lo stesso fingerprint.

L'elemento preso in input, è il contenuto dell'hard disk (o un file, un'immagine o qualunque altro elemento) che ricordiamo essere sempre e comunque una successione di bit; se si modifica anche solo uno di essi, il digest precedente e quello successivo alla modifica saranno notevolmente diversi. [2] In questo modo è facilmente riscontrabile se un supporto è stato alterato. Alcuni esempi di funzioni (o algoritmi) hash one-way, tutti egualmente utilizzati in ambito forense, sono: MD4, MD5, SHA-1. Vediamo l'algoritmo MD5 in dettaglio.

#### Algoritmo MD5

L'acronimo MD5 [3] indica un algoritmo crittografico di hashing realizzato da *Ronald Rivest* nel 1991. Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit (ovvero con lunghezza fissa di 32 valori esadecimali) che può essere usata per calcolare la firma digitale dell'input.

### 4.1.3 Mantenere la catena di custodia

Dovrebbe essere sempre mantenuta una corretta catena di custodia del reperto, ossia l'insieme delle azioni che lo hanno coinvolto, che devono essere opportunamente documentate. Il termine catena di custodia è infatti utilizzato per indicare il documento che contiene tutte le informazioni relative al reperto, dal momento dell'acquisizione (ciò che è stato fatto con la prova originale, ciò che è stato fatto con le copie forensi...), fino al giorno del processo.
Tipiche informazioni che possono essere lette su tale documento, sono: il nome dell'investigatore assegnatario del caso, data e ora di inizio della custodia, luogo di rinvenimento del supporto, caratteristiche tecniche dello

[2] A tale riguardo può essere utile consultare la Tabella 5.1.
[3] Message Digest Algorithm 5.

stesso. Ogni volta che uno dei supporti d'indagine viene assegnato ad un nuovo investigatore, al documento dovranno essere aggiunte le opportune informazioni.

## 4.2 Analisi: come procedere

L'analisi del reperto è la fase in cui si passa ad esaminare lo stesso per ricercare informazioni che potrebbero essere utili in sede processuale. Deve essere svolta su una copie forense dello stesso, utilizzando appositi strumenti software per analizzarne il contenuto. Molto spesso vengono utilizzati *toolkit* o distribuzioni forensi, che racchiudono al loro interno una collezione di software con precise funzionalità. Esistono sia suite commerciali (ne è un valido esempio *Encase*), che altrettanto valide distribuzioni open-source (*DEFT*, *Helix*, *Caine*...).

### 4.2.1 Gli elementi da ricercare

Grazie ai nuovi concetti introdotti, possiamo presentare una lista ampliata rispetto a quella riportata nel paragrafo 1.6.3, di ciò che il forenser si potrebbe trovare a dover analizzare: [Dftia]

- **Bad Blocks**, settori danneggiati del dispositivo;
- **Chat ed Instant Messaging**, le conversazioni tra gli utenti (alcuni programmi di Istant Messaging ne prevedono il salvataggio automatico);
- **Documenti ed immagini**, in un'ampia varietà di formati;
- **File cancellati**;
- **File cifrati**, le informazioni al loro interno non sono comprensibili a meno di non conoscerne la chiave. La crittanalisi è l'attacco alla crittografia, che mira ad estrarre i dati cifrati senza chiave;

- **File di log**;
- **File nascosti**;
- **File steganografati** mirano a celare l'esistenza di dati a chi non conosce la chiave atta ad estrarli. L'obiettivo della steganalisi è quello di dimostrare l'esistenza di tali dati, non di estrarli;
- **Navigazione web**, la cronologia, i cookie, i file scaricati dai siti visitati;
- **Partizioni cifrate o nascoste** con appositi software;
- **Posta elettronica**, scaricata sul computer tramite un gestore di posta o conservata sul server;
- **Registri di sistema**;
- **Slack Space** [Paragrafo 4.1.1].

### 4.2.2 Gli strumenti del mestiere

Avere uno o più dispositivi da esaminare offre un ampissimo spettro di possibilità in merito agli elementi da analizzare e alle modalità per farlo. Bisogna partire dal presupposto che, una volta garantita l'inalterabilità del reperto originale, non esistano procedure e stumenti migliori di altri, ma solamente un'insieme di dati che, se opportunamente trattato, potrebbe consentire di giungere a considerazioni interessanti. Per reperirli, un computer forenser potrebbe aver bisogno di software per:

- Il recupero di partizioni;
- Il recupero di dati cancellati;
- Recuperare dati da CD/DVD;
- Riparare i file corrotti;

- Recuperare le password;
- L'analisi del sistema;
- L'analisi del traffico di rete.

che solitamente sono di base contenuti in ogni toolkit forense.

### Un toolkit forense in dettaglio: DEFT

Il toolkit che è stato utilizzato per analizzare i risultati del progetto collegato a questa tesi è DEFT [4], una distribuzione live di software open-source utilizzabile a fini forensi. É un sistema operativo che utilizza come unica risorsa la memoria RAM, per questo motivo può essere utilizzato senza alterare in alcun modo le risorse della macchina su cui si sta eseguendo o dei dispositivi ad essa collegati.
Possiede anche una particolare funzionalità chiamata *DEFT-Extra* che, se eseguita su sistemi Windows, avvia un'interfaccia utente da cui è possibile selezionare una serie di applicativi utilizzabili sul sistema acceso (anche se

[4]Digital Evidence & Forensics Toolkit.


Figura 4.4: Schermata iniziale di deft-extra.

questo non è per nulla raccomandabile: il programma stesso mostra all'avvio un alert) [Figura 4.4].

#### Applicativi

Al suo interno sono presenti numerosi applicativi, molti dei quali di carattere open-source, che assolvono ai compiti più disparati. Per un elenco completo, si veda [FR09].

Le principali funzionalità utilizzate nella fase di analisi del progetto sono state:

- **Autopsy Forensic Browser** l'interfaccia grafica di *Sleuth Kit*. Principalmente è stata utilizzata la funzione *Timeline of File Activity* per ricostruire le movimentazioni subite dai file di sistema;
- **Md5sum** per il calcolo del digest del disco;
- **The Sleuth Kit** un software che consente di analizzare sistemi Windows e Unix.

## 4.3 Errori procedurali: il caso Garlasco

Citiamo nuovamente il caso Garlasco di cui si è discusso nel paragrafo 1.5.3, concentrandoci questa volta sulle mancanza di criterio nell'esecuzione di operazioni su uno dei reperti principali (il computer portatile di Alberto Stasi), che ha portato alla sua inammissibilità come prova.

### 4.3.1 L'accaduto

Il reperto, consegnato spontaneamente dall'indagato, è stato acceduto ripetutamente ed in maniera scorretta dalle stesse forze dell'ordine a cui era

stato affidato, prima dell'esecuzione di qualunque copia forense dello stesso. Riportiamo un estratto della sentenza in cui si annotano tali alterazioni [pen09]:

> *In data 14 agosto 2007 Stasi Alberto consegnava spontaneamente alla polizia giudiziaria il proprio computer portatile (marca "Compaq").*

Premettendo che, un reperto consegnato spontaneamente da un indagato dovrebbe richiedere un'attenzione anche maggiore del normale, così non è stato per il portatile di Stasi. Le forze dell'ordine a cui era stato affidato hanno operato maldestramente su di esso, senza prendere alcuna precauzione per salvaguardarne l'integrità.

> *Da quel momento fino al 29 agosto 2007, quando il reperto informatico veniva consegnato ai consulenti tecnici del pubblico ministero che procedevano all'effettuazione delle copie forensi dello stesso, i carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di indagine) alla quasi totalità del contenuto del computer.*

Tali operazioni, eseguite senza l'opportuna metodologia atta ad evitare l'alterazione dei dati presenti sul reperto, sono state solo parzialmente ammesse nei verbali giudiziari. Da un riscontro successivo sono risultate essere molto più consistenti:

> *Peraltro, già nel verbale di polizia giudiziaria datato 29 agosto 2007 i militari indicavano alcune delle operazioni condotte sul personal computer di Stasi. In realtà le metodologicamente scorrette attività espletate su tale fonte di prova sono risultate, all'esito dei successivi accertamenti tecnici, ancora più consistenti: sette (e non cinque come riferito) accessi al personal computer di Alberto Stasi; non corretta indicazione dell'avvenuta installazione ed utilizzo di diverse periferiche USB (oltre a quella correttamente indicata); non corretta indicazione dell'avvenuto accesso*

> *al disco esterno in uso ad Alberto Stasi; non corretta indicazione di accessi multipli al file della tesi di laurea in vari percorsi di memorizzazione dello stesso. [...]*

I consulenti tecnici del Pubblico Ministero hanno comunque proceduto all'analisi del reperto, desumendo che lo stesso veniva acceso ed utilizzato fino ad un determinato orario nella mattina in cui è avvenuto il delitto. Da quel momento in poi non sono state rinvenute altre tracce che dimostrino un'interazione attiva dell'utente sul computer portatile, che possano collocare Stasi al computer dopo quell'ora:

> *Il complesso di queste alterazioni veniva rilevato anche dai consulenti tecnici del pubblico ministero (i Ris di Parma) nella loro successiva analisi. Pur tenendo conto di quanto sopra, i Ris, nella loro relazione tecnica e successive integrazioni e chiarimenti, concludevano sostanzialmente nel senso che il giorno 13 agosto 2007 il computer portatile di Alberto Stasi veniva acceso alle ore 9.36; quindi venivano aperte delle fotografie digitali fino alle ore 9.57 e dopo le ore 10.17 non sarebbero presenti tracce informatiche che comportino la presenza attiva di un utente che interagisce con il PC.*

Tuttavia il consulente tecnico della difesa riscontrò la presenza di movimentazioni successive, nei file della tesi che Stasi stava scrivendo proprio in quei giorni. Tali informazioni, che avrebbero costituito un valido alibi per l'indagato, dovettero però essere eccepite come inutilizzabili proprio in merito alle alterazioni avvenute precedentemente all'analisi del reperto:

> *Il consulente tecnico della difesa, nel merito, evidenziava che in realtà il file della tesi era stato aperto alle ore 10.17 e che quella mattina erano state ivi scritte e memorizzate due pagine della tesi di laurea. In presenza tuttavia delle alterazioni al contenuto informativo della fonte di prova a causa degli accessi scorretti dei carabinieri e della ritenuta conseguente impossibilità di provare*

*con certezza quanto sopra rilevato, la difesa dell'imputato eccepiva l'inutilizzabilità come fonte di prova del contenuto del computer portatile in parola.*

### 4.3.2 Considerazioni

L'esecuzione di operazioni improprie su un reperto, in qualunque fase dell'indagine, ha come estrema conseguenza la sua inutilizzabilità come fonte di prova: le informazioni estratte dallo stesso saranno inservibili. É nell'interesse di tutte le parti del processo (accusa, difesa, parti civili...), che tutti gli elementi riscontrati possano essere liberamente utilizzati dalla corte in fase di giudizio. Qualunque minima alterazione che possa verificarsi durante lo svolgimento delle indagini influirebbe negativamente sull'ammissibilità in giudizio dell'elemento.
Per questo motivo ogni computer forenser dovrebbe sempre agire nel rispetto delle best practices, anche se queste non sono ancora, almeno in Italia, uno standard ufficiale.

Il progetto collegato a questa tesi, che verrà trattato nelle pagine successive [Capitoli 5 e 6] ha lo scopo di verificare le alterazioni che si verificano quando un reperto viene trattato impropriamente. L'esecuzione di determinati test su una copia forense dello stesso, determinerà una serie di alterazioni dei file del sistema che verranno opportunamente analizzate e confrontate.

# Capitolo 5

# Lo studio sperimentale

## 5.1 Descrizione dello studio

Questo progetto è stato intrapreso con l'obiettivo di analizzare in dettaglio le modifiche che avvengono sui file di un computer, al compimento di determinate operazioni. Sono stati perciò ideati ed eseguiti dei test, ossia delle combinazioni di azioni volutamente alla portata di tutti, che hanno lo scopo di imitare il comportamento di un qualunque utente di medio-basso livello, che adoperi un sistema operativo largamente diffuso, senza particolari personalizzazioni.
Per rendere il campo di analisi il più ampio possibile, sono state utilizzate immagini disco diverse per gruppi di test, per un totale di quattro (Img1, Img2, Img3 e Img4). Ognuna di esse rappresenta un diverso settaggio delle applicazioni in uso sul sistema operativo, nello specifico:

- **Scenario A:** la macchina analizzata è priva di qualunque protezione antivirus.
- **Scenario B:** la macchina possiede un software antivirus regolarmente aggiornato in cui sono stati mantenuti i settaggi di default.
- **Scenario C:** la macchina possiede un software antivirus regolarmente aggiornato in cui è impostata la scansione dell'intero sistema all'avvio.

- **Scenario D:** la macchina possiede un software antivirus regolarmente aggiornato in cui è impostata la scansione di tutti i dispositivi connessi.

Il passaggio immediatamente successivo all'esecuzione di ogni test è stato la raccolta dei dati. Per farlo, si è scelto di utilizzare un toolkit di applicazioni open-source: la distribuzione live DEFT [Paragrafo 4.2.2]. É stato così possibile, per ogni immagine testata, procedere al calcolo dell'hash, alla creazione di una *timeline* delle operazioni e all'estrazione di file ritenuti di qualche interesse (principalmente i log del sistema). Tutti i dati raccolti sono stati conseguentemente analizzati.
Importante notare che, per preservare l'indipendenza di ogni test, ognuno di essi è stato eseguito su una nuova copia bit-a-bit del sistema operativo di partenza [Figura 5.1].

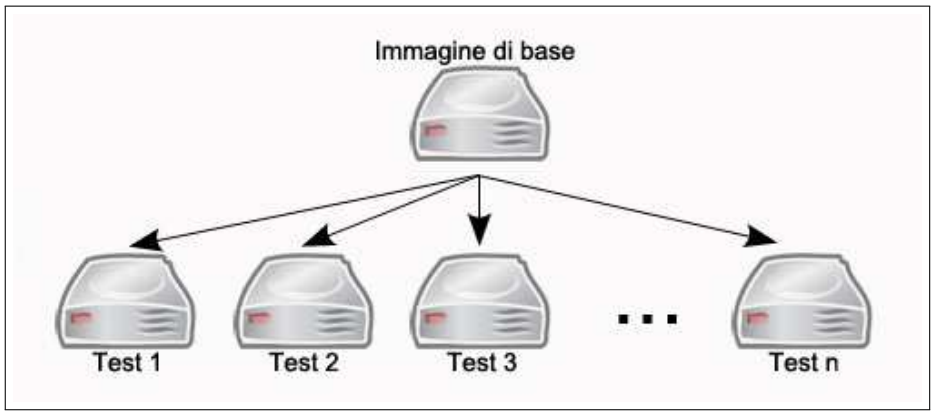



Figura 5.1: Rappresentazione dei criteri di virtualizzazione.

## 5.2 L'ambiente di virtualizzazione

Il progetto è stato condotto utilizzando un sistema di virtualizzazione al fine di poter facilmente ricreare l'ambiente voluto. L'utilizzo di questo strumento ha portato numerosi vantaggi sul piano pratico: ha consentito di snellire notevolmente le procedure di creazione e duplicazione delle immagini

utilizzate, di azzerare i costi relativi ai supporti di memorizzazione e di non essere legati materialmente ad un hardware che, anche se molto diffuso, potrebbe risultare quasi obsoleto.
Il software che si è scelto di utilizzare per lo scopo è *Oracle VM VirtualBox* (o semplicemente *VirtualBox*), ossia un programma open-source che consente di emulare la maggior parte dei sistemi operativi Windows e Linux. Consente una virtualizzazione totale, ossia una situazione in cui l'ambiente emulato risulta essere completamente svincolato dall'hardware della macchina che lo ospita.
Le sue caratteristiche combaciavano perfettamente con le esigenze di progetto. Particolarmente utili, da questo punto di vista, sono state la piena compatibilità con le porte USB e la possibilità di condividere una cartelle tra la macchina reale e quella virtuale, per poter facilmente passare i file da un'ambiente all'altro.
É stato utilizzato nella versione 4.1.0 r73009, sul sistema *Windows 7 Professional SP1*.

## 5.3 L'ambiente virtualizzato

### 5.3.1 Sistema operativo

Sulla Virtual Machine da 7 GB, creata tramite VirtualBox, è stato scelto di installare il sistema operativo *Windows XP Professional Sp1*. La scelta è ricaduta su questo sistema perchè, oltre alla ridotta quantità di spazio richiesto su disco e alla piena compatibilità con gli applicativi odierni, è ancora il più diffuso al mondo [1]. É stata utilizzata la versione in lingua inglese fornita agli studenti del *Dipartimento di Scienze dell'Informazione* dell'*Università di Bologna*, dal *MSDN academic alliance software center*.
Sono stati creati due utenti, uno con privilegi di amministratore "Admin" e l'altro standard "User1", entrambi protetti da una semplice password: "ad-

[1] 50,5% di diffusione tra tutti i sistemi operativi per computer desktop, a Settembre 2011 [*Web Metrics*].

min" per il primo e "user" per il secondo. Infine sono stati disabilitati gli aggiornamenti automatici.

### 5.3.2 Software installato

Successivamente sulla Virtual Machine sono stati installati determinati applicativi, vediamoli in dettaglio:

- **Adobe Reader X** è un software freeware, liberamente scaricabile dal sito di *Adobe*, ed è tra i più diffusi del suo genere. Permette di aprire, consultare e stampare i file in formato pdf.
  É stato installato nella versione 10.1.1.

- **Avast! Free Antivirus [non presente su Img1]** è il terzo software antivirus più diffuso al mondo [2]. Le sue funzionalità più rilevanti, sono la scansione dell'intero sistema o di specifiche cartelle e l'aggiornamento automatico delle definizioni, e del programma, anche più volte al giorno.
  É stato installato nella versione 6.0.1289.0.

- **Microsoft Office Professional Edition 2003** è la nota suite proprietaria di applicativi per l'ufficio. I software compresi al suo interno sono: *Word* (un word processor), *Excel* (un foglio di calcolo), *PowerPoint* (creazione e gestione di presentazioni), *Access* (gestione di database), *Publisher* (creazione di elaborati grafici e non) e *Outlook* (gestione di posta elettronica e rubrica).
  É stato installato nella versione 11.0.8173.0.

- **Microsoft Internet Explorer** è il web browser più diffuso a livello mondiale [3]. La pagina principale impostata è about:blank.
  Non è stata necessaria l'installazione in quanto il software era già compreso sul sistema operativo.

[2] Al terzo posto con l'8,66%, dopo *Microsoft Security Essentials* (10,66%) e *Avira Antivir Personal* (10,18%) [*OPSWAT*].

[3] 47,07% di diffusione a giugno 2011 [*StatCounter*]. [Stati]

- **Mozilla Firefox** è il secondo web browser più diffuso a livello mondiale [4]. La pagina principale impostata è about:blank.
  É stato installato nella versione 5.0.1.

- **OpenOffice.org** è la suite open-source di applicativi per l'ufficio sviluppata da *Oracle Corporation*, rivale per eccellenza di *Microsoft Office*. I software che la compongono sono: *Writer* (un word processor), *Calc* (un foglio di calcolo), *Draw* (programma di grafica vettoriale), *Impress* (creazione e gestione di presentazioni), *Math* (editor di formule matematiche) e *Base* (gestione di database).
  É stato installato nella versione 3.3.

Sono inoltre state installate 2 stampanti, di cui una virtuale:

- **HP Deskjet F2420** stampante a getto d'inchiostro della casa HP. Per installarla è stato utilizzato il driver HP Deskjet F2400 All-in-one 14.0 Rel 6 scaricato dal sito del produttore.

- **PDF creator** è un software open-source sviluppato dalla comunità di *pdfforge*, che consente di creare file pdf da qualsiasi applicazione. Permette di gestire le sue funzionalità come se fosse una stampante, aggiungendo la voce *PDFCreator* alle stampanti selezionabili dal computer. É stato installato nella versione 1.2.2.

Per tutti i software precedentemente elencati sono state mantenute le configurazioni di default, ed ognuno di essi è stato avviato almeno una volta per regolarizzare la prima richiesta di registrazione del prodotto.

### 5.3.3 File preesistenti

Per completare lo scenario, all'interno della cartella Documenti di ogni utente sono stati inseriti 5 files per ogni formato principale: .doc, .xls, .ppt, .pdf, .txt, .jpg, .png, .gif e .mp3. I file sono tutti diversi gli uni dagli altri per titolo e contenuto.

[4] 30,36% di diffusione a giugno 2011 [*StatCounter*]. [Stati]


Figura 5.2: Elenco dei file presenti nella cartella Documenti.

## 5.4 Immagini forensi utilizzate per i test

Come accennato in precedenza, si sono voluti ricreare quattro possibili scenari di utilizzazione di un computer. Per questo motivo sono state create altrettante diverse immagini disco, che differiscono tra di loro o per il software installato, o per le configurazioni di quest'ultimo. In generale, possiamo dire che le immagini sono una l'evoluzione dell'altra, con la prima che è stata utilizzata per creare la seconda, e quest'ultima che è stata utilizzata a sua volta per creare la terza e la quarta [Figura 5.3]. Vediamole in dettaglio.

### 5.4.1 Img1

Rappresenta l'immagine di partenza, utilizzata come base di tutte le altre. Sono state mantenute tutte le impostazioni di default, e il sistema è stato lasciato volutamente sprovvisto di qualunque forma di protezione (antivirus e non). Sono stati inoltre disattivati gli aggiornamenti automatici di Windows.

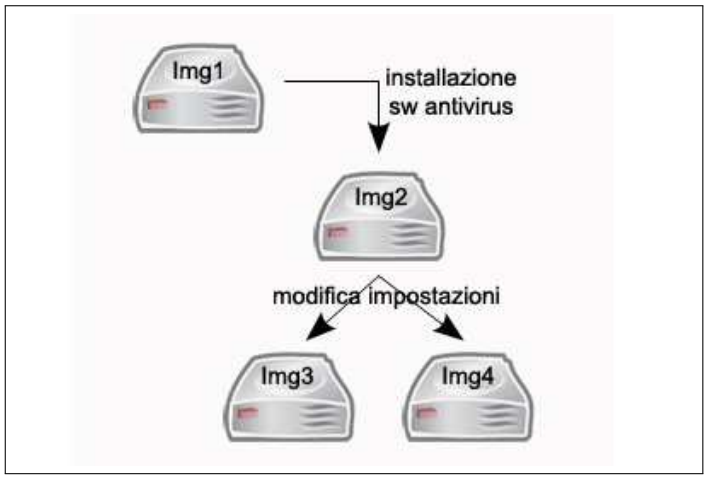



Figura 5.3: Schema di creazione delle immagini forensi.

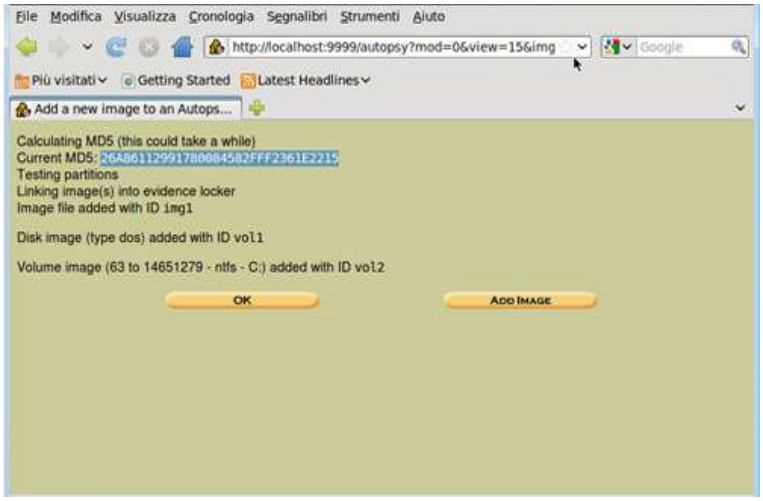
Dopo l'installazione ed il primo avvio di tutte le applicazioni, l'immagine è stata "congelata", ovvero utilizzata come base per tutti i test successivi. A garanzia, ne è stato calcolato l'hash utilizzando l'algoritmo *MD5*, che risulta quindi essere: 26a86112991780084582fff2361e2215.

### 5.4.2 Img2

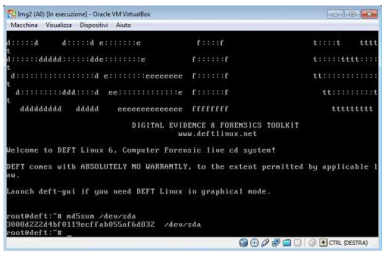
Tutti i software di Img1 sono installati anche su questa macchina, con l'unica aggiunta di *Avast! Free Antivirus*. Sono state mantenute le stesse impostazioni di default, sia per le applicazioni precedenti, che per l'antivirus. Anche questa immagine è stata congelata dopo la sua preparazione, e l'MD5 calcolato su di essa è: 3008d222d4bf0119ecffab055af6d832.

### 5.4.3 Img3

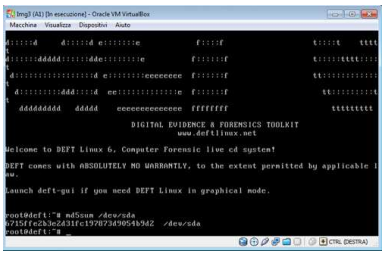
Presenta una sola differenza rispetto a Img2: *Avast! Free Antivirus* è stato impostato per la scansione dell'intero sistema all'avvio.
L'MD5 calcolato su di essa è: 6715ffe2b3e2d31fc197873d9054b9d2.



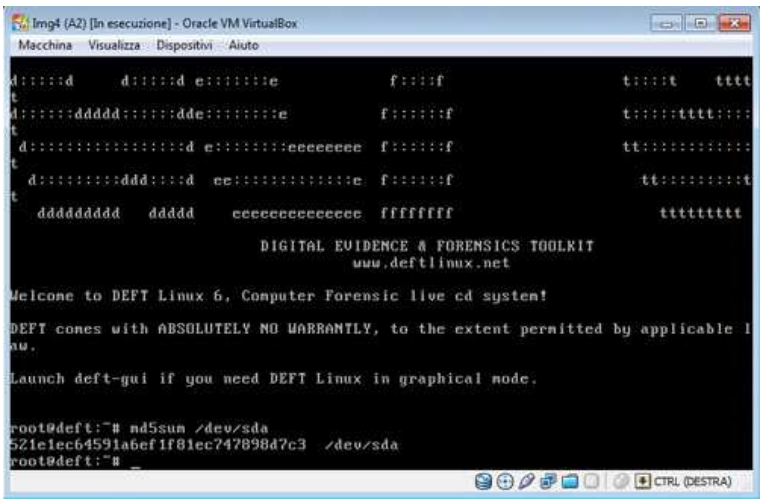

(a) Digest di Img1



(b) Digest di Img2



(c) Digest di Img3




(d) Digest di Img4


Figura 5.4: Schermata di Avast! per la scelta della modalità di scansione.

### 5.4.4 Img4

Anche questa immagine presenta una singola differenza rispetto a Img2, qui *Avast! Free Antivirus* è stato settato per eseguire automaticamente la scansione di tutti i dispositivi connessi.
Il suo MD5 è 521e1ec64591a6ef1f81ec747898d7c3.

## 5.5 Modalità ed esecuzione dei test

Viene di seguito riportata la lista integrale dei test eseguiti sulle diverse immagini forensi. Successivamente vengono riportate le modalità di esecuzione per ognuna di esse.

### 5.5.1 Elenco dei test

**Avviare la macchina:**

1. E spegnerla con unplugging mentre compare la schermata di caricamento di Windows;
2. E spegnerla con shutdown alla schermata di login;
3. E spegnerla con unplugging alla schermata di login;
4. E tentare l'accesso con l'utente amministratore sbagliando la password una volta, quindi spegnere con shutdown;
5. E tentare l'accesso con l'utente amministratore sbagliando la password una volta, quindi spegnere con unplugging;
6. E tentare l'accesso con l'utente amministratore sbagliando la password dieci volte, quindi spegnere con shutdown;
7. E tentare l'accesso con l'utente amministratore sbagliando la password dieci volte, quindi spegnere con unplugging;
8. E tentare l'accesso con l'utente standard sbagliando la password una volta, quindi spegnere con shutdown;
9. E tentare l'accesso con l'utente standard sbagliando la password una volta, quindi spegnere con unplugging;
10. E tentare l'accesso con l'utente standard sbagliando la password dieci volte, quindi spegnere con shutdown;
11. E tentare l'accesso con l'utente standard sbagliando la password dieci volte, quindi spegnere con unplugging;
12. Con l'utente amministratore senza sbagliare la password, quindi spegnere con shutdown;
13. Con l'utente amministratore senza sbagliare la password, quindi spegnere con unplugging;

14. Con l'utente standard senza sbagliare la password, quindi spegnere con shutdown;

15. Con l'utente standard senza sbagliare la password, quindi spegnere con unplugging;

16. Con utente amministratore e lasciarla accesa per almeno 15 minuti senza fare niente, quindi spegnere con shutdown;

17. Con utente amministratore e lasciarla accesa per almeno 30 minuti senza fare niente, quindi spegnere con shutdown;

18. Con utente amministratore e lasciarla accesa per almeno 60 minuti senza fare niente, quindi spegnere con shutdown;

19. Con utente amministratore e lasciarla accesa per almeno 120 minuti senza fare niente, quindi spegnere con shutdown;

20. Con utente standard e lasciarla accesa per almeno 15 minuti senza fare niente, quindi spegnere con shutdown;

21. Con utente standard e lasciarla accesa per almeno 30 minuti senza fare niente, quindi spegnere con shutdown;

22. Con utente standard e lasciarla accesa per almeno 60 minuti senza fare niente, quindi spegnere con shutdown;

23. Con utente standard e lasciarla accesa per almeno 120 minuti senza fare niente, quindi spegnere con shutdown.

**Avviare la macchina e accedere come utente amministratore (al termine spegnere sempre con shutdown).**

24. Aprire e chiudere Word;

25. Aprire e chiudere Excel;

26. Aprire e chiudere Powerpoint;

27. Aprire e chiudere Internet Explorer;
28. Aprire e chiudere Mozilla Firefox;
29. Aprire e chiudere Acrobat Reader;
30. Aprire e chiudere Writer;
31. Aprire e chiudere Calc;
32. Aprire e chiudere Impress;
33. Aprire Word, scrivere qualcosa, chiudere il documento senza salvarlo (facendo il tutto in pochi secondi);
34. Aprire Word, scrivere qualcosa, chiudere il documento senza salvarlo (facendo il tutto in più di 10 minuti. [5]);
35. Aprire un file di Word esistente e chiuderlo (facendo il tutto in pochi secondi);
36. Aprire un file di Word esistente, inviare la stampa e chiuderlo;
37. Aprire Paint, disegnare qualcosa e chiudere senza salvare;
38. Aprire un'immagine jpg, inviare la stampa e chiuderla;
39. Visitare il sito di Google con Internet Explorer;
40. Visitare il sito di Google con Mozilla Firefox;
41. Utilizzando la funzione cerca di Windows, cercare la parola *keyword_di_test_1* su tutto il disco C;
42. Utilizzando la funzione cerca di Windows, cercare la parola *keyword_di_test_1* limitandosi alla cartella "documenti";
43. Copiare un file dalla cartella "documenti" al desktop;
44. Collegare una chiavetta USB e poi scollegarla correttamente via software;

[5] Tempo impostato di default per l'esecuzione di salvataggi automatici.

45. Collegare una chiavetta USB, aprire un file salvato su di essa e richiuderlo, poi scollegare la chiave USB correttamente via software;

46. Collegare una chiavetta USB, creare una cartella su di essa, scollegare la chiave USB correttamente via software;

47. Collegare una chiavetta USB, copiare i file presenti nella cartella "documenti" sulla chiave USB, poi scollegarla correttamente via software.

### 5.5.2 Modalità di esecuzione

Prendendo a riferimento l'elenco del paragrafo precedente:

- Su Img1 sono stati eseguiti tutti i test, dal numero 1 al 47 compreso;
- Su Img2, Img3 e Img4 è stato identificato ed eseguito un sottoinsieme dei test più significativi, ossia i numeri:
  2 - 6 - 10 - 12 - 14 - 16 - 20 - 35 - 39 - 41 - 44.

## 5.6 Calcolo dell'MD5

Per dimostrare che delle modifiche sono intervenute durante ogni test, sull'immagine usata è stato calcolato l'MD5. L'elenco dei digest ottenuti è riportato a fronte, nella Tabella 5.1.
Tale tabella è molto utile al giurista per comprendere che, variando anche un solo bit, l'hash di un'immagine disco cambia completamente. Per le proprietà viste al Paragrafo 4.1.2, la minima variazione genera ogni volta un hash totalmente diverso dal precedente.

Tabella 5.1: Elenco dei digest

| | Img1 | | 934d04058784c222fb8bd2ae28feadf0 |
|---|---|---|---|
| 1 | bcef52fa12d154bb6056d2158248ab0b | 42 | 65c15bc1f74d16cd9fba5621ae832092 |
| 2 | 6c29af1704fdd2c035191c17d0d3be40 | 43 | e6c1701f995449d893ab162fca0babbe |
| 3 | b10517d5d244cfe5c8c2bc3d1986338b | 44 | e630998bfa2478723b249dc95f1b39bc |
| 4 | 123311267954497cc52d30583d6cfa9a | 45 | cb98a14007be27e521f1af8e0ef41880 |
| 5 | 799845156f7ac46efd4c91c7dba58654 | 46 | 5adfbf4cc729437c6d6d944d1e2aafdb |
| 6 | fe0c9e8adb09b092e6f314bb8d876a41 | 47 | 364152fbb525ffda83de814e75b898a7 |
| 7 | e15ec3702aec217b9b75c06ec6c00685 | | Img2 |
| 8 | 5bb45043e1a93d870fab8b67111dd476 | 6 | 8c76741a34c86136fb1834c324009442 |
| 9 | b6f234645071b47c843314f1b2c62988 | 10 | 4014bc5dc61da423d2d087d31fe192fa |
| 10 | 2ea304df1e35c85aa3e3ebd5bf3681bd | 12 | ebdee6a639d68df15a8056b8f36d667b |
| 11 | 1d4c1f82b7498ae588d51e1db7ed534a | 14 | 697ec5c2f5800a07c04ff4e7058fce37 |
| 12 | c470f6635f80e25768534731efadb7fa | 16 | 87a20d6853b4794e35674876e6449768 |
| 13 | 8ec1a97b6ea8bc5b83b610256e8701e5 | 20 | f46053eff8fa6affbd80c984c611f1e1 |
| 14 | bf1d89341176b815693699a5f2b21a18 | 35 | df8aa8e2618db5c3464757d3914cf577 |
| 15 | e29c94827a403bc642a51aaba8c759cb | 39 | 44211fada4aa9b19f9988be934551bed |
| 16 | 71d79ee02f080c625a5b0b49b49ec1e2 | 41 | 2452c9129f0f79ded72215fdc91c4c1f |
| 17 | 01bb0e94a8725ae56076a3ede6ed5ccb | 44 | daa6c7e23b6e6a30db79f46fcfb4547f |
| 18 | 2e77cf9bde2008d84a9b85d4050ad322 | | Img3 |
| 19 | 7cfda83572856fccfb457b41f70813e9 | 6 | 51bbf12991de4ffc51feb17340166fbb |
| 20 | 221f98cf675329d06e54aed3a5430e9e | 10 | db4a7382afaf97dd056ce139c60efe09 |
| 21 | a8e598b8ffdb0de460704eb8bb689aa0 | 12 | b009440faa62919b3386b6edda8fb4ae |
| 22 | c04a841b67fc40092c75d9c52d1c01ab | 14 | 9989e0216178b955b8393d83bbf4da23 |
| 23 | 2dd1f90656f4c31fd3026ccdacc05d86 | 16 | ce8057a12cb546c2c8f53d66873225ca |
| 24 | 4f488dc0cd0f3e430b27ae0bb6736c06 | 20 | 5a3c09e8684f9a7ac6b2d7afbde622d1 |
| 25 | a8842fbcf88b30636393872a8c36f28a | 35 | f86ea97b2e748c8eb22d25446f9f6247 |
| 26 | 971dd8522f3275be7ba4e830ec471396 | 39 | 5ccb24d19369f03a6278d5ffdbbef058 |
| 27 | ff99c774d0930299701aed8864125cdc | 41 | 65d4e30ba144aabb105f0b118b2484ac |
| 28 | 0ccad24c56b0c17d7a81cfc68636d83d | 44 | ff4d0602e0840984fb3df705448eba81 |
| 29 | a62503149495922d784fa9b04d0b2055 | | Img4 |
| 30 | b515f97fa918efc2d8527700d0a7c8e1 | 2 | 3b46253011c8d0a4cd7186509dae5fc1 |
| 31 | e9b1517c48f275fab65cee73e6e1b0d5 | 6 | 6ccbe5230b99708b235c65589cc3e530 |
| 32 | f164458fd8d2d9e1147ab08af509c7bb | 10 | 651ecffe31ac7178df98b456f6448754 |
| 33 | 550062faed2de77497d543d6e5419689 | 12 | 6a72c4b9b3d0e8f74ab8bb416f8fa1fd |
| 34 | ea74d732595a5c0cb4bcfc73a869f68d | 14 | 8d7616fb002da10a40179766b7251ea4 |
| 35 | 97bf4967c9bfce345fb9a835ea676560 | 16 | 4d48e825992dbbfc499bff2d73cb9352 |
| 36 | c3e216aefd0b3d14709d2f155a23e9f8 | 20 | ffa998fb4c3b8703583ba7254b138f9e |
| 37 | b7ae9ff6633057e520766fe6b4d52834 | 35 | f576eb0292a04fe599a6a2f999f9b296 |
| 38 | 70a9e68ccf40ee8cca713ddd67c9f9c5 | 39 | 8058a40c495ab299ad21cae19697b477 |
| 39 | 190f87930fbdba39ee60b7ed19a8ccea | 41 | 98404f4819234689ebf98957e9b1222d |
| 40 | 632e1e24ef5f45639b4d8267de4b235a | 44 | fae9e5f4c4d8eb114c69b1e520e506eb |

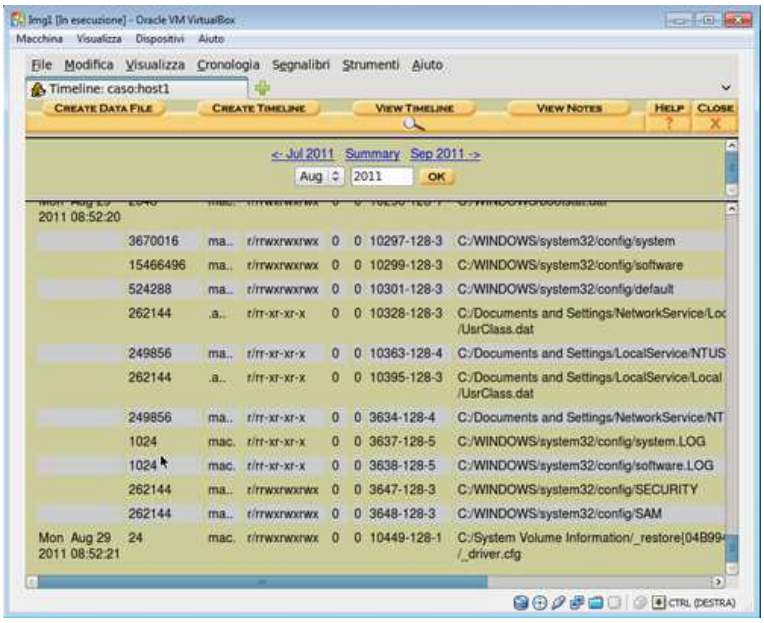



Figura 5.5: Ultime operazioni rilevate su Img1, prima del congelamento

## 5.7 Analisi delle timeline

Per generare la timeline di ciascun test è stato utilizzato il tool *Autopsy Forensic Browser*, presente all'interno di DEFT. Ovviamente ogni timeline è stata creata partendo da una definizione temporale ben chiara, che comprendesse solamente i movimenti avvenuti durante l'esecuzione del test, ignorando tutte le operazioni riguardanti la creazione e configurazione della stessa immagine.
Le ultime operazioni riscontrate su Img1, prima del congelamento, sono mostrate alla Figura 5.5.

### 5.7.1 Lettura della timeline

La stuttura della timeline è di facile comprensione, ogni sua entry rappresenta una specifica azione avvenuta su un file, ovvero: accesso, modifica del contenuto, modifica dei metadati o creazione dello stesso.

Prendiamo la seguente voce come esempio:

```
Wed Sep 28 2011 15:52:13 56 .a.. d/drwxrwxrwx 0 0 10358-144-5 C:/Documents and Settings/Admin
```

Procediamo ad analizzare le sue componenti [CARti]:

- **Data e ora** dell'attività (o del gruppo di attività). Nell'esempio: Wed Sep 28 2011 15:52:13.
- **Dimensione** del file letto e/o modificato e/o creato. Nell'esempio: 56(kb).
- **Tipo di operazione**, è specificato da una lettera ("m", "a", "c" o "b") o una combinazione di esse; per il loro significato si rimanda ai sotto-paragrafi 5.7.1.1 e 5.7.1.2. Nell'esempio: ".a..".
- **Permessi (mode)**, l'insieme delle operazioni consentite su quel determinato file. [6] Nell'esempio: d/drwxrwxrwx.
- **User identifier (UID)**, è un valore numerico che identifica univocamente un utente del sistema (sui sistemi Win è sempre settato a 0).
- **Group identifier (GID)**, è un valore numerico che identifica un gruppo di utenti del sistema (sui sistemi Win è sempre settato a 0).
- **Indirizzo dei metadati** nella MFT [7]. Nell'esempio: 10358-144-5.
- **Percorso del file**. Per i files cancellati, compare la dicitura "(deleted)" alla fine, e per quelli che puntano ad uno spazio già riallocato, la dicitura "(realloc)". Nell'esempio: C:/Documents and Settings/Admin.

[6] Si presenta come una stringa di lunghezza dieci, così composta: in prima posizione si ha "d" se è una directory o "-" se è un file. La seconda, terza e quarta lettera rappresentano i permessi dell'utente ("r" se è leggibile, "w" se è modificabile, "x" se è esegubile). La quinta, sesta e settima lettera sono i permessi del gruppo di utenti. Le ultime tre lettere sono infine i permessi per chiunque acceda da altre posizioni.

[7] Master File Table (nei volumi con file system NTFS), è un database relazionale che conserva vari attributi relativi ai files, ed è di fatto una sorta di tavola dei contenuti del volume.

### Tipi di movimento

I movimenti possibili dipendono dal file system del sistema che si sta analizzando [CARti]:

- Per i sistemi *UNIX* (file system *EXT2* e *EXT3*), le voci possibili sono:
  - **"m" modified** il file è stato modificato.
  - **"a" accessed** la data di ultimo accesso al file è cambiata.
  - **"c" changed** l'inode[8] è stata modificata. Il file è stato presumibilmente sovrascritto.
- Per i sistemi *DOS* e *Windows* fino alla versione *ME* (file system *FAT*), abbiamo:
  - **"m" written** il file è stato modificato.
  - **"a" accessed** la data di ultimo accesso al file è cambiata.
  - **"c" created** Il file è stato creato.
- E infine, per i sistemi appartenenti alla famiglia *Windows NT* [9] (file system *NTFS*), abbiamo:
  - **"m" written** il file è stato modificato.
  - **"a" accessed** il file è stato acceduto
  - **"c" changed** i metadati (relativi al file) presenti nella MFT sono stati modificati.
  - **"b" created** il file è stato creato.

Visto che la macchina testata monta il sistema operativo Windows XP (file system NTFS), ci troviamo nell'ultimo caso.

[8] Nei sistemi UNIX è la struttura del file system che ne archivia le informazioni.

[9] Ossia Windows 3.1, Windows 2000, Windows XP, Windows Vista e Windows 7, nonchè le server edition.

Tabella 5.2: Tipologie di movimento previste per File System

| File system | m | a | c | b |
|---|---|---|---|---|
| EXT | modified | accessed | changed | - |
| FAT | written | accessed | created | - |
| NTFS | written | accessed | changed | created |

### Ricostruzione delle operazioni

Come accennato nel paragrafo precedente, le operazioni rilevabili sui file sono di base quattro (ricordiamo: modifica, accesso, modifica dei metadati, e creazione), anche combinabili tra loro, per un totale di 15 combinazioni. Nella Figura 5.6 tratta da [HAL98], sono mostrati alcuni esempi di possibili interpretazioni delle operazioni registrate.

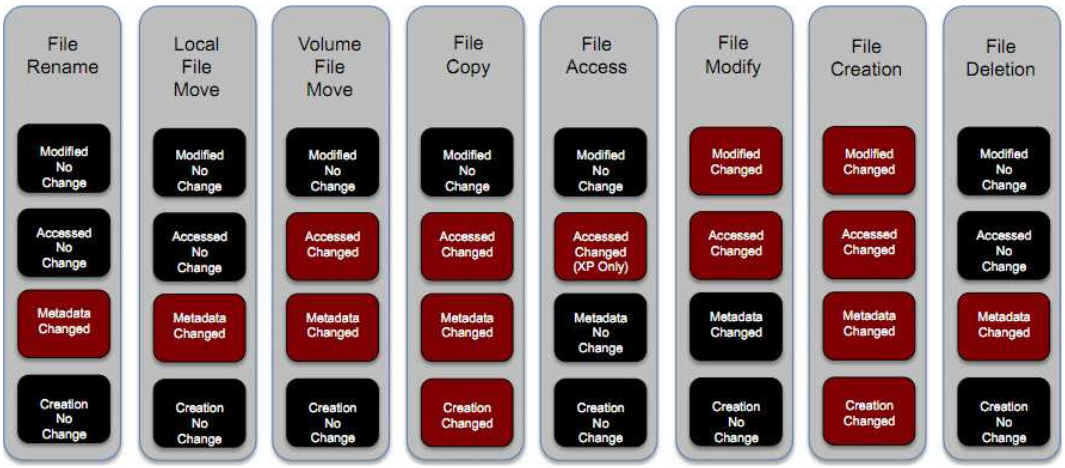



Figura 5.6: Timeline: esempi di ricostruzione delle operazioni.

# Capitolo 6

# Analisi dei risultati ottenuti

## 6.1 Dati estratti dalle timeline

Vengono di seguito presentati alle pagine 76 e 77, i dati raccolti dall'analisi delle timeline. La lettura delle tabelle è abbastanza intuitiva: per ogni test (il numero di riferimento è riportato nella prima colonna) sono elencate le ricorrenze di ogni tipologia di operazione rilevata. L'ultima colonna contiene invece la somma di quelle precedenti, ossia il totale delle operazioni registrate per quello specifico test.

Successivamente alla pagina 78, sono riportate le tabelle riepilogative degli stessi movimenti. Questi sono stati raggruppati per tipologia di operazione base, ossia accesso (a), modifica (m), modifica dei metadati (c) o creazione (b). Ogni operazione è stata considerata indipendentemente dalle altre.

Tabella 6.1: Risultati dei test eseguiti su Img1

| # | .a.. | ma.. | m... | ..c. | mac. | macb | m.c. | ...b | .ac. | m..b | ma.b | .a.b | m.cb | ..cb | .acb | TOT. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 1 |
| 2 | 819 | 5 | - | 17 | 50 | 2 | 3 | - | - | - | - | - | - | - | - | 896 |
| 3 | 511 | - | - | 8 | 9 | - | 8 | - | - | - | - | - | - | - | - | 536 |
| 4 | 818 | 6 | - | 17 | 50 | 2 | 3 | - | - | - | - | - | - | - | - | 896 |
| 5 | 658 | - | - | 12 | 12 | - | 9 | - | - | - | - | - | - | - | - | 691 |
| 6 | 867 | 6 | - | 17 | 52 | 2 | 3 | - | - | - | - | - | - | - | - | 947 |
| 7 | 861 | - | - | 18 | 42 | 1 | 11 | 1 | - | - | - | - | - | - | - | 934 |
| 8 | 1.101 | 6 | - | 17 | 50 | 1 | 4 | 1 | - | - | - | - | - | - | - | 1.180 |
| 9 | 1.002 | - | - | 4 | 8 | - | 7 | - | - | - | - | - | - | - | - | 1.021 |
| 10 | 1.149 | 6 | - | 17 | 48 | 2 | 6 | - | - | - | - | - | - | - | - | 1.228 |
| 11 | 1.149 | - | - | 18 | 41 | 2 | 11 | - | - | - | - | - | - | - | - | 1.221 |
| 12 | 1.317 | 7 | - | 29 | 61 | 6 | 5 | 1 | 4 | 1 | - | - | - | - | - | 1.431 |
| 13 | 1.178 | - | - | 29 | 35 | 4 | 13 | 1 | 4 | - | - | - | - | - | - | 1.264 |
| 14 | 1.435 | 7 | - | 99 | 64 | 4 | 6 | 4 | 8 | - | - | - | - | - | - | 1.627 |
| 15 | 1.277 | - | - | 98 | 36 | 3 | 13 | 2 | 9 | - | - | - | - | - | - | 1.438 |
| 16 | 1.326 | 8 | 3 | 36 | 68 | 6 | 4 | 1 | 4 | - | 1 | - | - | - | - | 1.457 |
| 17 | 1.324 | 8 | 3 | 35 | 69 | 6 | 3 | 1 | 5 | - | 1 | - | - | - | - | 1.455 |
| 18 | 1.416 | 9 | 3 | 36 | 74 | 37 | 13 | 6 | 8 | - | 1 | 8 | 1 | - | - | 1.612 |
| 19 | 1.443 | 9 | - | 32 | 79 | 38 | 22 | 6 | 8 | - | - | 8 | 1 | - | - | 1.646 |
| 20 | 1.446 | 8 | 6 | 109 | 69 | 6 | 1 | 1 | 8 | - | 1 | - | - | - | - | 1.655 |
| 21 | 1.534 | 9 | 3 | 107 | 77 | 36 | 12 | 6 | 10 | - | - | 8 | 1 | - | - | 1.803 |
| 22 | 1.537 | 9 | 3 | 108 | 77 | 34 | 15 | 9 | 10 | - | - | 8 | 1 | - | - | 1.811 |
| 23 | 1.621 | 9 | 3 | 108 | 87 | 39 | 15 | 6 | 9 | - | - | 8 | 1 | - | - | 1.906 |
| 24 | 1.359 | 7 | - | 30 | 67 | 7 | 4 | 2 | 5 | - | - | - | - | - | - | 1.481 |
| 25 | 1.371 | 7 | - | 30 | 70 | 14 | 5 | 2 | 7 | - | - | - | 1 | - | - | 1.507 |
| 26 | 1.355 | 7 | - | 29 | 66 | 5 | 5 | 2 | 6 | - | - | - | - | - | - | 1.475 |
| 27 | 1.371 | 8 | 2 | 37 | 75 | 113 | 7 | 8 | 6 | - | - | 1 | - | - | - | 1.628 |
| 28 | 1.470 | 8 | - | 33 | 80 | 15 | 9 | 3 | 5 | - | - | 1 | - | - | - | 1.624 |
| 29 | 1.363 | 8 | - | 28 | 66 | 6 | 5 | 2 | 6 | - | - | - | - | - | - | 1.484 |
| 30 | 1.490 | 8 | - | 34 | 67 | 9 | 9 | 1 | 3 | - | - | - | 3 | - | - | 1.624 |
| 31 | 1.490 | 7 | - | 30 | 69 | 11 | 5 | 1 | 4 | 1 | - | - | 2 | - | - | 1.620 |
| 32 | 1.508 | 7 | - | 31 | 69 | 10 | 7 | - | 5 | - | - | - | 3 | - | - | 1.640 |
| 33 | 1.353 | 7 | - | 28 | 70 | 10 | 4 | 2 | 7 | - | - | - | - | - | - | 1.481 |
| 34 | 1.415 | 8 | - | 33 | 75 | 19 | 8 | 1 | 6 | - | - | - | - | - | - | 1.565 |
| 35 | 1.386 | 7 | 3 | 38 | 77 | 12 | 5 | 4 | 7 | - | - | - | - | - | - | 1.539 |
| 36 | 1.406 | 7 | 3 | 39 | 72 | 13 | 7 | 2 | 6 | - | - | 2 | - | - | - | 1.557 |
| 37 | 1.371 | 8 | - | 29 | 66 | 6 | 4 | 2 | 6 | - | - | - | - | - | - | 1.492 |
| 38 | 1.383 | 7 | - | 30 | 69 | 12 | 6 | 3 | 9 | - | - | 1 | - | - | - | 1.520 |
| 39 | 1.370 | 8 | 2 | 38 | 78 | 128 | 6 | 10 | 6 | - | - | - | - | - | - | 1.646 |
| 40 | 1.462 | 8 | 3 | 33 | 83 | 16 | 4 | 5 | 6 | - | - | 1 | - | - | - | 1.621 |
| 41 | 15.245 | 8 | 3 | 93 | 71 | 5 | 7 | 1 | 18 | - | - | - | - | - | - | 15.451 |
| 42 | 1.429 | 7 | 4 | 91 | 66 | 5 | 4 | 3 | 17 | - | - | - | - | - | - | 1.626 |
| 43 | 1.365 | 7 | 3 | 35 | 65 | 6 | 6 | 2 | 5 | - | - | - | - | - | - | 1.494 |
| 44 | 1.326 | 8 | 3 | 42 | 70 | 7 | 4 | 3 | 6 | - | - | - | - | - | - | 1.469 |
| 45 | 1.384 | 8 | 3 | 41 | 75 | 11 | 3 | 2 | 8 | - | - | - | - | - | - | 1.535 |
| 46 | 1.373 | 8 | 3 | 50 | 62 | 5 | 7 | 1 | 4 | - | - | 1 | - | - | - | 1.514 |
| 47 | 1.408 | 8 | 3 | 43 | 70 | 8 | 4 | 1 | 9 | - | - | - | - | - | - | 1.554 |

Tabella 6.2: Risultati dei test eseguiti su Img2

| # | .a.. | ma.. | m... | ..c. | mac. | macb | m.c. | ...b | .ac. | m..b | ma.b | .a.b | m.cb | ..cb | .acb | TOT. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1.307 | 6 | - | 12 | 37 | 6 | 5 | - | 4 | - | - | - | - | - | - | 1.377 |
| 6 | 1.764 | 7 | 7 | 24 | 80 | 7 | 6 | 8 | 11 | - | - | - | - | - | - | 1.914 |
| 10 | 1.807 | 8 | 4 | 21 | 80 | 8 | 7 | 6 | 12 | - | - | - | - | - | - | 1.953 |
| 12 | 1.838 | 9 | 8 | 36 | 81 | 6 | 5 | 4 | 11 | - | - | - | - | - | - | 1.998 |
| 14 | 1.844 | 10 | 6 | 36 | 80 | 5 | 7 | 4 | 10 | - | - | - | - | - | - | 2.002 |
| 16 | 2.027 | 35 | 11 | 41 | 93 | 15 | 8 | 8 | 13 | - | - | - | - | 43 | - | 2.294 |
| 20 | 2.032 | 35 | 13 | 41 | 96 | 15 | 9 | 9 | 19 | - | - | - | - | 42 | - | 2.311 |
| 35 | 1.936 | 8 | 4 | 39 | 96 | 16 | 9 | 5 | 15 | - | - | - | - | - | - | 2.128 |
| 39 | 1.880 | 9 | 5 | 45 | 92 | 105 | 8 | 5 | 12 | - | - | - | - | - | - | 2.161 |
| 41 | 15.822 | 34 | 12 | 112 | 107 | 13 | 8 | 19 | 26 | - | - | - | - | 36 | - | 16.189 |
| 44 | 1.889 | 8 | 2 | 42 | 87 | 8 | 8 | 3 | 12 | - | 1 | - | - | - | 1 | 2.061 |

Tabella 6.3: Risultati dei test eseguiti su Img3

| test | .a.. | ma.. | m... | ..c. | mac. | macb | m.c. | ...b | .ac. | m..b | ma.b | .a.b | m.cb | ..cb | .acb | TOT. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1.715 | 6 | - | 12 | 48 | 3 | 5 | 2 | 4 | - | - | 1 | 1 | - | - | 1.797 |
| 6 | 1.811 | 41 | 12 | 29 | 92 | 13 | 12 | 13 | 10 | - | - | - | - | 40 | 1 | 2.074 |
| 10 | 1.779 | 7 | 1 | 20 | 94 | 7 | 7 | 10 | 10 | - | - | - | - | - | - | 1.935 |
| 12 | 1.840 | 8 | 1 | 30 | 85 | 8 | 8 | 6 | 11 | - | - | 1 | - | - | - | 1.998 |
| 14 | 1.838 | 8 | 2 | 31 | 83 | 7 | 6 | 6 | 6 | - | - | - | - | - | - | 1.987 |
| 16 | 2.067 | 35 | 9 | 49 | 123 | 15 | 7 | 11 | 13 | - | - | - | - | 42 | - | 2.371 |
| 20 | 1.784 | 36 | 8 | 43 | 118 | 17 | 9 | 9 | 16 | - | - | - | - | 42 | - | 2.082 |
| 35 | 1.677 | 9 | - | 38 | 124 | 22 | 12 | 6 | 14 | - | - | - | - | - | - | 1.902 |
| 39 | 1.947 | 9 | 2 | 41 | 126 | 106 | 11 | 13 | 14 | - | - | 1 | - | - | - | 2.270 |
| 41 | 15.785 | 10 | 6 | 102 | 125 | 10 | 7 | 11 | 27 | - | - | - | - | - | - | 16.083 |
| 44 | 1.908 | 8 | - | 44 | 114 | 11 | 11 | 6 | 13 | - | - | - | - | - | - | 2.115 |

Tabella 6.4: Risultati dei test eseguiti su Img4

| # | .a.. | ma.. | m... | ..c. | mac. | macb | m.c. | ...b | .ac. | m..b | ma.b | .a.b | m.cb | ..cb | .acb | TOT. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1.715 | 8 | - | 21 | 72 | 4 | 7 | 2 | 8 | - | - | - | - | - | - | 1.837 |
| 6 | 1.775 | 7 | - | 20 | 77 | 7 | 7 | 5 | 10 | - | - | - | - | - | - | 1.908 |
| 10 | 1.775 | 7 | - | 20 | 77 | 7 | 7 | 5 | 10 | - | - | - | - | - | - | 1.908 |
| 12 | 1.820 | 8 | - | 31 | 84 | 10 | 12 | 3 | 13 | - | - | - | - | - | - | 1.981 |
| 14 | 1.848 | 8 | 3 | 31 | 87 | 10 | 8 | 3 | 16 | - | - | - | - | - | - | 2.014 |
| 16 | 2.042 | 10 | 3 | 45 | 103 | 16 | 9 | 9 | 14 | - | - | - | - | 41 | - | 2.292 |
| 20 | 2.053 | 10 | 4 | 49 | 105 | 17 | 6 | 9 | 12 | - | - | - | - | 40 | - | 2.305 |
| 35 | 1.915 | 8 | - | 38 | 99 | 14 | 12 | 4 | 13 | - | - | - | 1 | - | - | 2.104 |
| 39 | 1.940 | 10 | 2 | 44 | 108 | 112 | 7 | 10 | 12 | - | - | - | - | - | - | 2.245 |
| 41 | 15.804 | 8 | 3 | 100 | 108 | 12 | 8 | 7 | 23 | - | - | - | - | - | - | 16.073 |
| 44 | 1.906 | 8 | 3 | 47 | 97 | 9 | 4 | 5 | 10 | - | - | 1 | - | - | - | 2.090 |

Tabella 6.5: Risultati raggruppati per tipo di movimento (Img1)

| Test | a | m | c | b | Test | a | m | c | b |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | - | - | - | 25 | 1.469 | 97 | 127 | 17 |
| 2 | 876 | 60 | 72 | 2 | 26 | 1.439 | 83 | 111 | 7 |
| 3 | 520 | 17 | 25 | - | 27 | 1.574 | 205 | 238 | 122 |
| 4 | 876 | 61 | 72 | 2 | 28 | 1.579 | 112 | 142 | 19 |
| 5 | 670 | 21 | 33 | - | 29 | 1.449 | 85 | 111 | 8 |
| 6 | 927 | 63 | 74 | 2 | 30 | 1.577 | 96 | 125 | 13 |
| 7 | 904 | 54 | 72 | 2 | 31 | 1.581 | 95 | 121 | 15 |
| 8 | 1.158 | 61 | 72 | 2 | 32 | 1.599 | 96 | 125 | 13 |
| 9 | 1.010 | 15 | 19 | - | 33 | 1.447 | 91 | 119 | 12 |
| 10 | 1.205 | 62 | 73 | 2 | 34 | 1.523 | 110 | 141 | 20 |
| 11 | 1.192 | 54 | 72 | 2 | 35 | 1.489 | 104 | 139 | 16 |
| 12 | 1.395 | 80 | 105 | 8 | 36 | 1.506 | 102 | 137 | 17 |
| 13 | 1.221 | 52 | 85 | 5 | 37 | 1.457 | 84 | 111 | 8 |
| 14 | 1.518 | 81 | 181 | 8 | 38 | 1.481 | 94 | 126 | 16 |
| 15 | 1.325 | 52 | 159 | 5 | 39 | 1.590 | 222 | 256 | 138 |
| 16 | 1.413 | 90 | 118 | 8 | 40 | 1.576 | 114 | 142 | 22 |
| 17 | 1.413 | 90 | 118 | 8 | 41 | 15.347 | 94 | 194 | 6 |
| 18 | 1.553 | 138 | 169 | 53 | 42 | 1.524 | 86 | 183 | 8 |
| 19 | 1.585 | 149 | 180 | 53 | 43 | 1.448 | 87 | 117 | 8 |
| 20 | 1.538 | 91 | 193 | 8 | 44 | 1.417 | 92 | 129 | 10 |
| 21 | 1.674 | 138 | 243 | 51 | 45 | 1.486 | 100 | 138 | 13 |
| 22 | 1.675 | 139 | 245 | 52 | 46 | 1.453 | 85 | 128 | 7 |
| 23 | 1.773 | 154 | 259 | 54 | 47 | 1.503 | 93 | 134 | 9 |
| 24 | 1.445 | 85 | 113 | 9 | | | | | |

Tabella 6.6: Risultati raggruppati per tipo di movimento (Img2, Img3, Img4)

| Img2 | | | | | Img3 | | | | | Img4 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Test | a | m | c | b | Test | a | m | c | b | Test | a | m | c | b |
| 2 | 1.360 | 54 | 64 | 6 | 2 | 1.777 | 63 | 73 | 7 | 2 | 1.807 | 91 | 112 | 6 |
| 6 | 1.968 | 170 | 197 | 67 | 6 | 1.968 | 170 | 197 | 67 | 6 | 1.876 | 98 | 121 | 12 |
| 10 | 1.897 | 116 | 138 | 17 | 10 | 1.897 | 116 | 138 | 17 | 10 | 1.876 | 98 | 121 | 12 |
| 12 | 1.945 | 109 | 139 | 10 | 12 | 1.953 | 110 | 142 | 15 | 12 | 1.935 | 114 | 150 | 13 |
| 14 | 1.949 | 108 | 138 | 9 | 14 | 1.942 | 106 | 133 | 13 | 14 | 1.969 | 116 | 152 | 13 |
| 16 | 2.183 | 162 | 213 | 66 | 16 | 2.253 | 189 | 249 | 68 | 16 | 2.185 | 141 | 228 | 66 |
| 20 | 2.197 | 168 | 222 | 66 | 20 | 1.971 | 188 | 245 | 68 | 20 | 2.197 | 142 | 229 | 66 |
| 35 | 2.071 | 133 | 175 | 21 | 35 | 1.846 | 167 | 210 | 28 | 35 | 2.049 | 134 | 177 | 19 |
| 39 | 2.098 | 219 | 262 | 110 | 39 | 2.203 | 254 | 298 | 120 | 39 | 2.182 | 239 | 283 | 122 |
| 41 | 16.002 | 174 | 302 | 68 | 41 | 15.957 | 158 | 271 | 21 | 41 | 15.955 | 139 | 251 | 19 |
| 44 | 2.006 | 114 | 158 | 13 | 44 | 2.054 | 144 | 193 | 17 | 44 | 2.031 | 121 | 167 | 15 |

## 6.2 Peso percentuale delle operazioni rilevate

Servendoci di alcune rappresentazioni grafiche, osserviamo in alcuni test significativi il peso percentuale delle diverse tipologie di operazioni (solamente le principali: accesso, modifica del file e modifica dei metadati) rispetto al totale dei file presenti sull'immagine dopo l'esecuzione del relativo test. Questo numero, ad esempio, sull'immagine Img1 congelata si aggira intorno ai 20'000 file.

### Analisi dei risultati del test 2

Il grafico 6.1, mostra il peso percentuale delle operazioni rilevate dopo l'esecuzione del test 2, ossia *avvio della macchina con spegnimento alla schermata di login.*
La legenda va interpretata in questo modo: (1), files acceduti, (2) files modificati, (3) files di cui sono stati modificati i metadati e (4) files che, per differenza, non sono stati toccati [1].

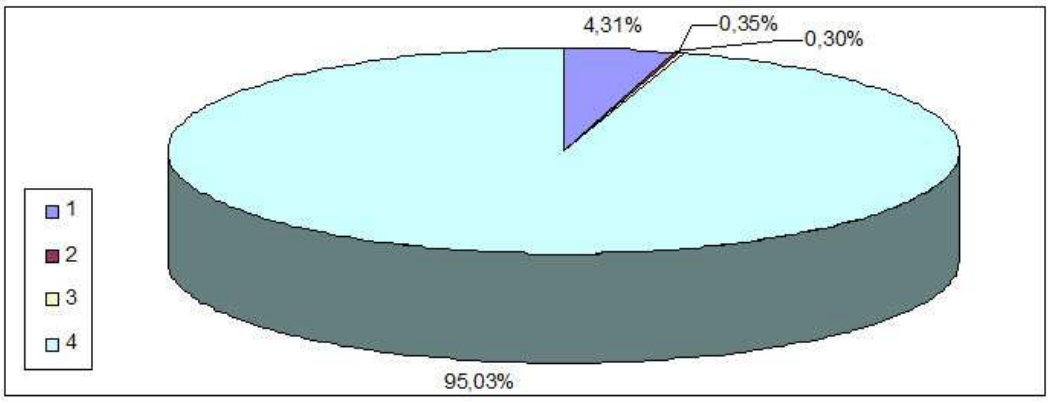



Figura 6.1: Test 2: peso percentuale delle operazioni rilevate.

[1] Si tratta di una stima, in quanto non è possibile determinare con assoluta certezza quanti e quali file non siano mai stati movimentati dal sistema.

### Analisi dei risultati del test 39

Il grafico 6.2, mostra il peso percentuale delle operazioni rilevate dopo l'esecuzione del test 39, ossia *la visita del sito di Google tramite Internet Explorer*.
La legenda va interpretata in questo modo: (1), files acceduti, (2) files modificati, (3) files di cui sono stati modificati i metadati e (4) files che, per differenza, non sono stati toccati.

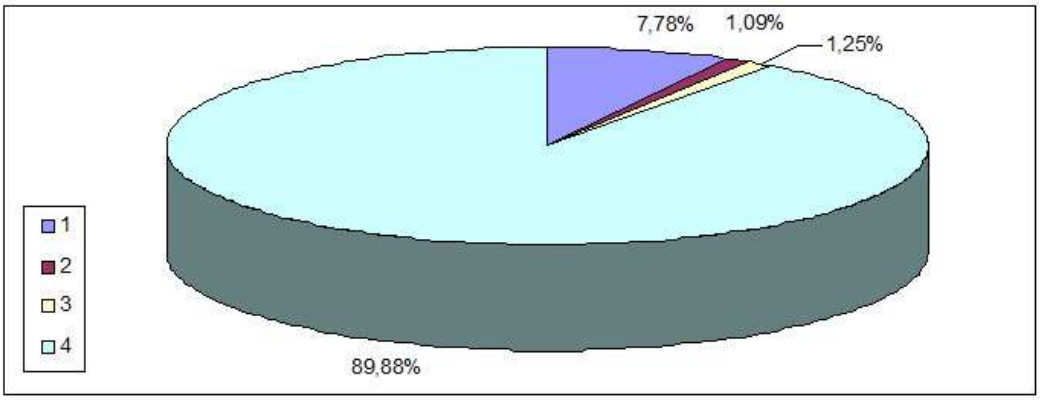



Figura 6.2: Test 39: peso percentuale delle operazioni rilevate.

### Analisi dei risultati del test 41

Il grafico 6.3, mostra il peso percentuale delle operazioni rilevate dopo l'esecuzione del test 41, ossia *ricerca di una parola chiave su C: tramite l'utilizzo della funzione "Cerca"*.
La legenda va interpretata in questo modo: (1), files acceduti, (2) files modificati, (3) files di cui sono stati modificati i metadati e (4) files che, per differenza, non sono stati toccati.

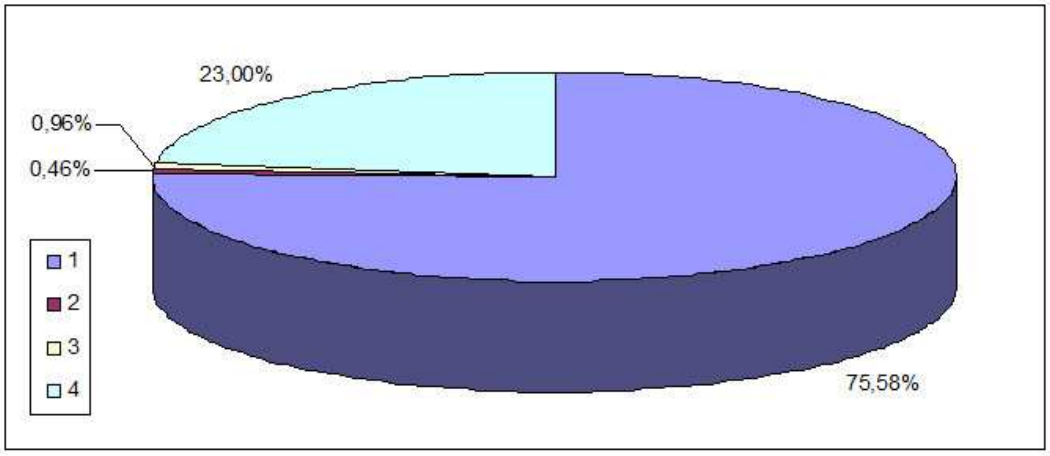



Figura 6.3: Test 41: peso percentuale delle operazioni rilevate.

## 6.3 Comparazione dei risultati

Servendoci di alcuni grafici, in questo capitolo ci dedicheremo alla comparazione dei dati raccolti. [2] In particolar modo, ci soffermeremo sulle differenze tra modalità di spegnimento, tipologie di account, funzionamento di software concorrenti e funzionamento delle diverse modalità antivirus.

### 6.3.1 Sulle modalità di arresto: unplugging e shutdown

#### Spegnimento alla schermata di login

Prendiamo in esame i test 2 e 3 eseguiti su Img1, ossia *avvio della macchina con spegnimento alla schermata di login.* Come possiamo osservare nella Figura 6.4, l'intuizione di scollegare una macchina (test 3), invece di arrestarla con procedura standard (test 2), è corretta. Con l'unplugging il numero dei files acceduti e quello dei modificati è notevolmente più basso.
É stata rilevata una differenza di 360 movimentazioni.

[2] Sono stati considerati i dati più significativi delle tabelle 6.1, 6.2, 6.3 e 6.4.

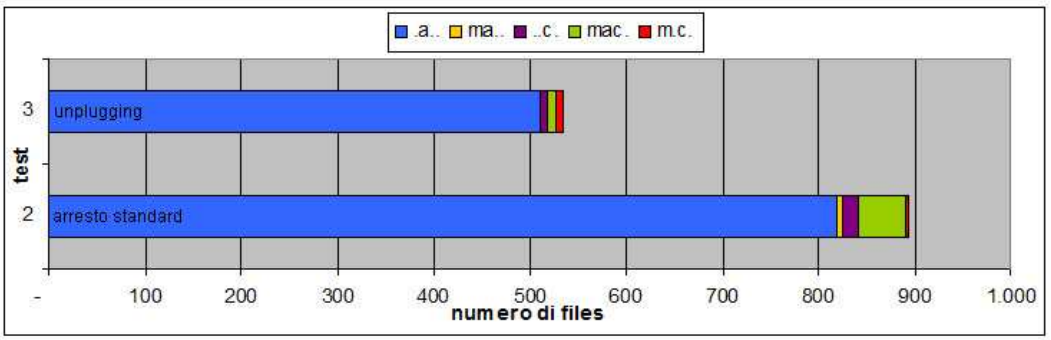



Figura 6.4: Unplugging VS Shutdown - spegnimento alla schermata di login.

### Digitazione password errata

Prendiamo in esame i test 4 e 5 eseguiti su lmg1, ossia *digitazione errata della password di Admin (una volta).*
Nella Figura 6.5 possiamo osservare che, anche in questo caso, con la procedura di unplugging (test 5) le movimentazioni di accesso e modifica sono notevolmente minori rispetto allo spegnimento con shutdown (test 4).
É stata rilevata una differenza di 205 operazioni.

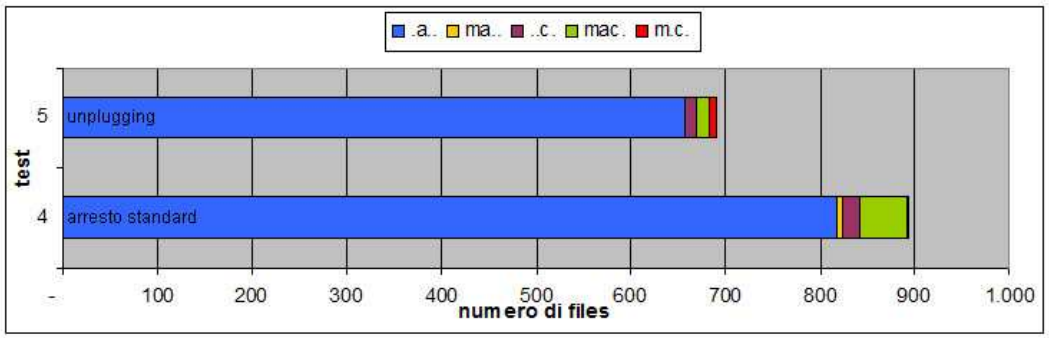



Figura 6.5: Unplugging VS Shutdown - digitazione password errata.

### Digitazione password corretta

Prendiamo in esame i test 12 e 13 eseguiti su lmg1, ossia *accesso al sistema dopo la digitazione corretta della password di Admin.*
Anche in questo caso (Figura 6.6) vale quanto riferito nei due test precedenti: l'unplugging (test 13) registra meno modificazioni rispetto allo spegnimento con shutdown (test 12). Questa volta la differenza di operazioni risulta essere 167.

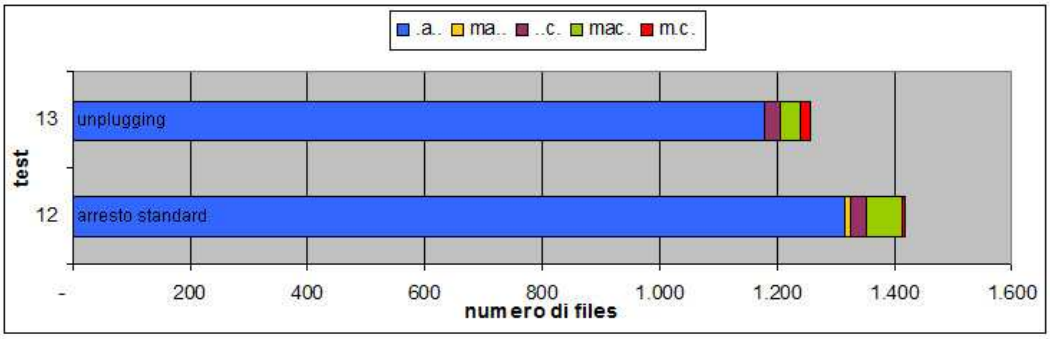



Figura 6.6: Unplugging VS Shutdown - digitazione password corretta.

### Conclusioni

La procedura standard di arresto (shutdown) registra sempre un numero maggiore di movimentazioni rispetto all'unplugging. La differenza media rilevata (sui test esaminati) è di circa 240 file coinvolti tra operazioni di accesso, modifica e creazione.

## 6.3.2 Sulla tipologia di utente: admin e standard user

### Digitazione password errata

Prendiamo in esame i test 5 e 9 eseguiti su lmg1, ossia *digitazione errata della password (una volta).*

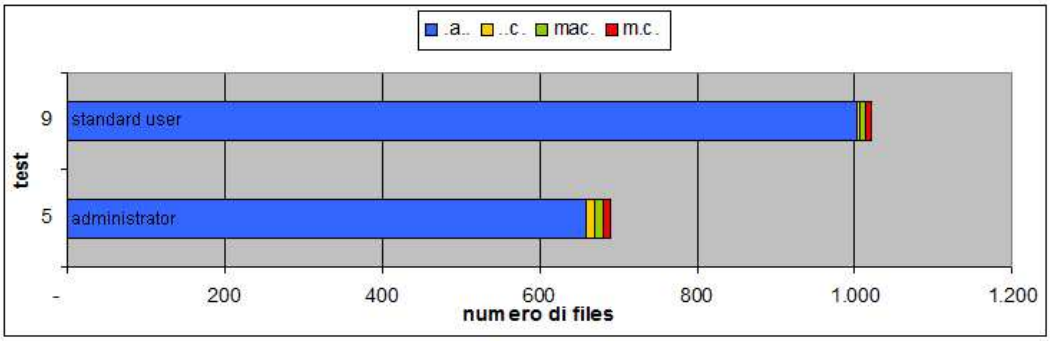



Figura 6.7: Admin VS utente standard - digitazione password errata.

Nella Figura 6.7, osserviamo che le operazioni eseguite sull'utente standard (test 9) sono di molto superiori (di quasi 1/3) a quelle eseguite sull'utente amministratore (test 5). L'utente amministratore ha però un numero leggermente più elevato di movimentazioni relative alla creazione di files.
É stata rilevata una differenza di 330 movimentazioni.

### Digitazione password corretta

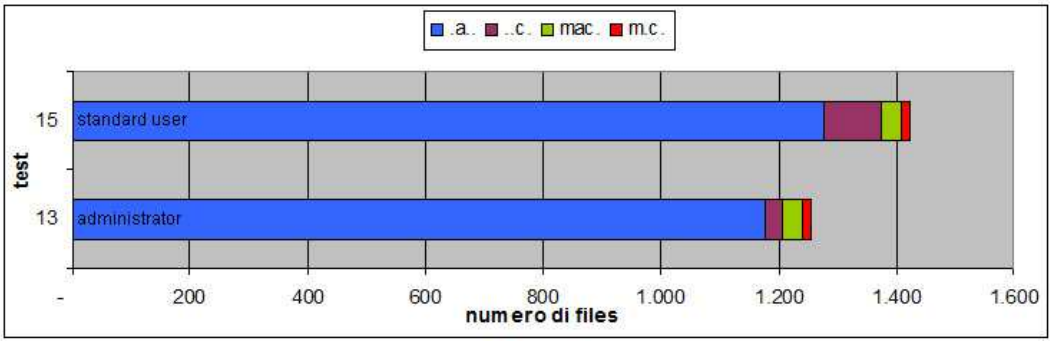



Figura 6.8: Admin VS utente standard - digitazione password corretta.

Prendiamo in esame i test 13 e 15 eseguiti su Img1, ossia *digitazione corretta della password*. Nella Figura 6.8 possiamo osservare che le movimentazioni registrate sull'utente standard (test 15) sono di poco superiori;

le differenze più evidenti si notano nuovamente sui files acceduti. Nell'utente amministratore (test 13) sono però stati riscontrati il triplo di files creati. Questa volta la differenza delle operazioni risulta essere 174.

### Macchina accesa e inutilizzata per 30 minuti

Prendiamo in esame i test 17 e 21 eseguiti su lmg1, ossia *macchina lasciata accesa e inutilizzata per 30 minuti.*
Anche in questo caso, la situazione illustrata precedentemente si ripete: l'utente standard (test 21) registra un numero molto superiore di files acceduti e files creati (..c. e macb), rispetto all'utente amministratore (test 17). Gli altri valori risultato essere costanti.
É stata rilevata una differenza di 348 operazioni.

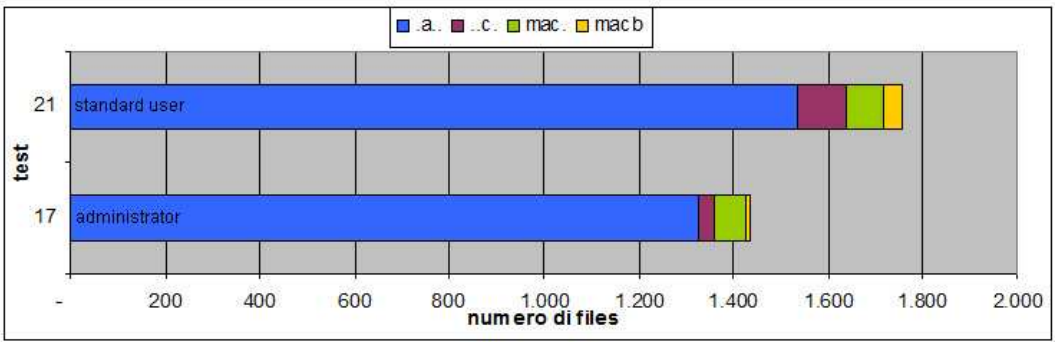



Figura 6.9: Admin VS utente standard - macchina accesa per 30 minuti.

### Conclusioni

Utilizzare un'utente standard rispetto ad un utente amministratore registra sempre un numero maggiore di movimentazioni. La differenza media rilevata (sui test esaminati) è di circa 240 file coinvolti tra operazioni di accesso, modifica e creazione.

### 6.3.3 Sul software utilizzato

Passiamo ora alla comparazione dei software installati; in particolar modo verranno trattate le suite di prodotti per l'ufficio e i browser.

#### Suite per l'ufficio

Mettiamo a confronto le alterazioni che potrebbero derivare da uno scorretto uso delle più conosciute suite di prodotti per l'ufficio disponibili oggi sul mercato: *Microsoft Office* e *OpenOffice.org*. Come già accennato nel capitolo precedente, ognuna di esse è una raccolta di applicativi, con usi e funzionalità specifiche.
Prendiamo in esame i tre prodotti più rilevanti di ciascuna: *Word* e *Writer* (test 24 e 30), *Excel* e *Calc* (test 25 e 31), *PowerPoint* e *Impress* (test 26 e 32), *avviati e poi chiusi sull'account di admin*. Nella Figura 6.10 possiamo osservare che, di base, i prodotti OpenOffice.org (test 30, 31 e 31) registrano quasi 1/3 di operazioni in più rispetto ai rivali (test 24, 25 e 26). Tale incremento avviene sui files acceduti; i restanti dati sono costanti a parte lievi oscillazioni dei files macb.

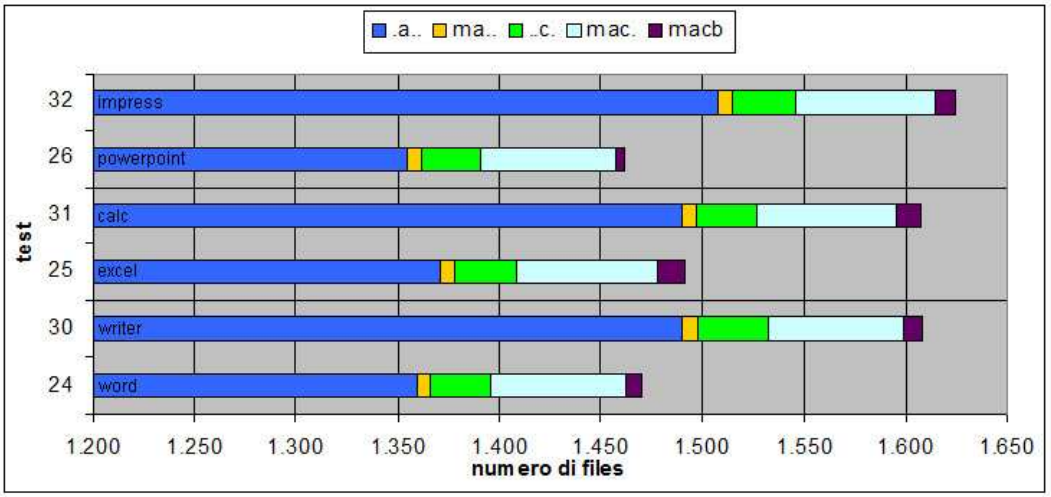



Figura 6.10: Software - avvio e chiusura degli applicativi di Office e OpenOffice.

### Browser

Prendiamo in esame i test 39 e 40 eseguiti su lmg1, ossia *la visita del sito di google con il browser*.
Nella Figura 6.11 possiamo osservare che, anche se la differenza totale tra le operazioni dei due test non è particolarmente rilevante, le situazioni sono notevolmente diverse. Mozilla Firefox (test 40) supera Internet Explorer sul numero di files acceduti (quasi 1/3 di più). Internet Explorer (test 39) invece registra un numero maggiore di operazioni macb. Le uniche voci costanti risultano essere ..c. e mac.

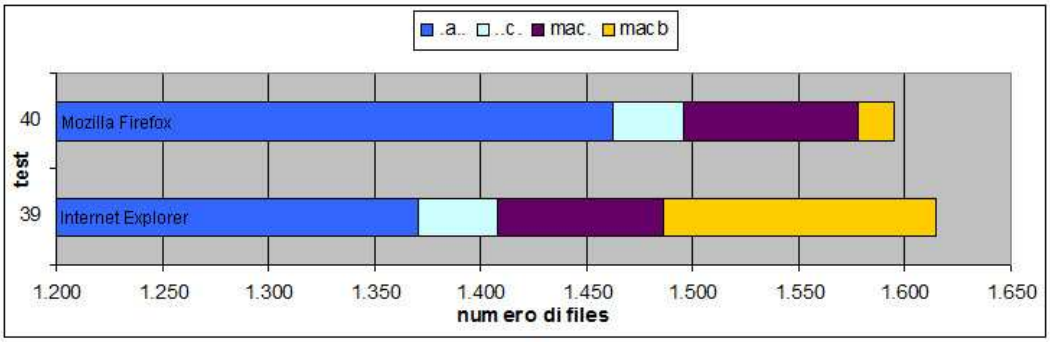



Figura 6.11: Software - utilizzo dei browser Internet Explorer e Mozilla Firefox.

## 6.3.4 Sui settaggi del software antivirus

Passiamo ora al confronto di immagini diverse, che ricordiamo differiscono tra loro solamente per le diverse impostazioni (o l'assenza) del programma antivirus.

### Spegnimento alla schermata di login

Consideriamo il test 2 eseguito su tutte le quattro immagini, ossia *spegnimento alla schermata di login*.
Osservando la Figura 6.12 possiamo notare come il numero di files acceduti

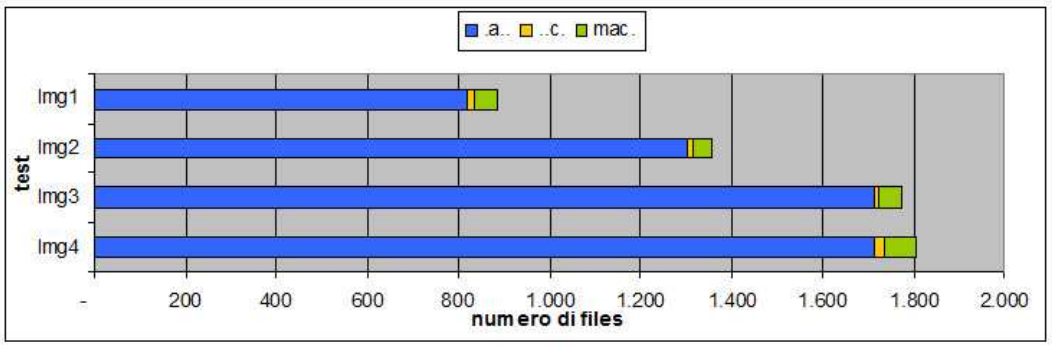



Figura 6.12: Antivirus - spegnimento alla schermata di login.

aumenti prograssivamente. Poca è la variazione di tutte le altre tipologie di movimento.

### Digitazione password errata (10 volte)

Consideriamo il test 6 eseguito su tutte le quattro immagini, ossia *digitazione password errata (10 volte)*. Osservando la Figura 6.13 possiamo notare che la variazione più rilevante sia sempre quella legata ai files acceduti (che risultano raddoppiare quando è installato un sw antivirus). Le operazioni ma.. raggiungono il loro punto di massimo su Img3. Le altre variazioni possono considerarsi abbastanza costanti.

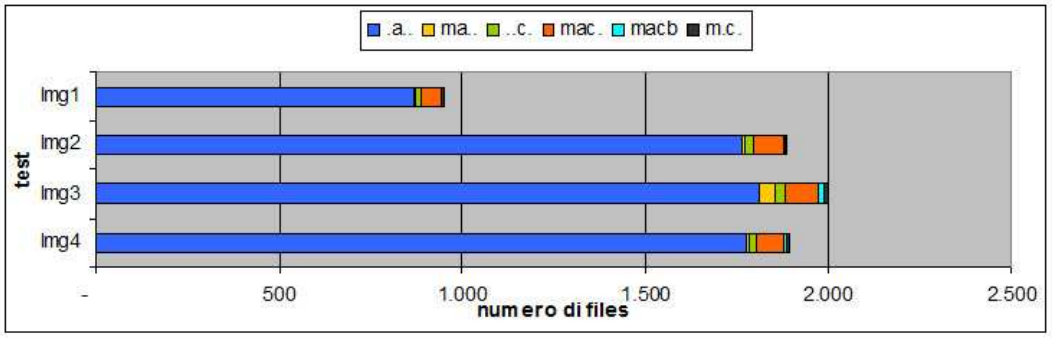



Figura 6.13: Antivirus - digitazione password errata (10 volte).

### Digitazione password corretta

Consideriamo il test 12 eseguito su tutte le quattro immagini, ossia *digitazione password corretta di admin.*
Nella Figura 6.14 possiamo osservare che a variare sono principalmente i files acceduti, che compiono un balzo notevole quando è installato un sw antivirus. Le altre operazioni sono costanti.

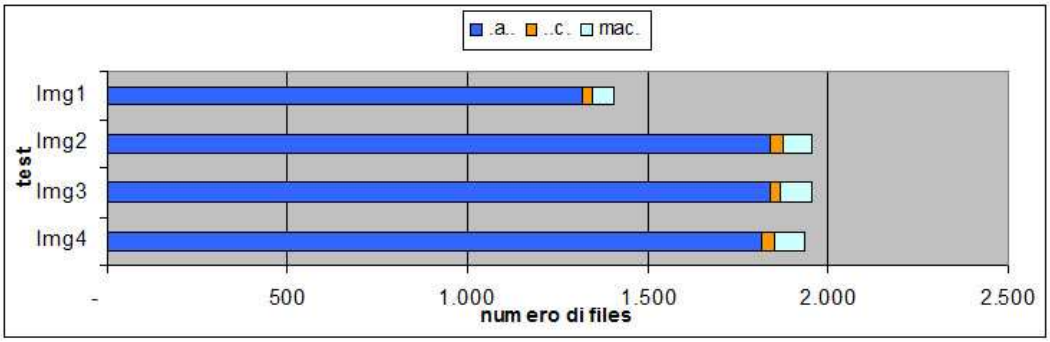



Figura 6.14: Antivirus - digitazione password corretta.

### Macchina accesa e inutilizzata per 15 minuti

Consideriamo il test 16 eseguito su tutte le quattro immagini, ossia *macchina lasciata accesa e inutilizzata per 15 minuti.*

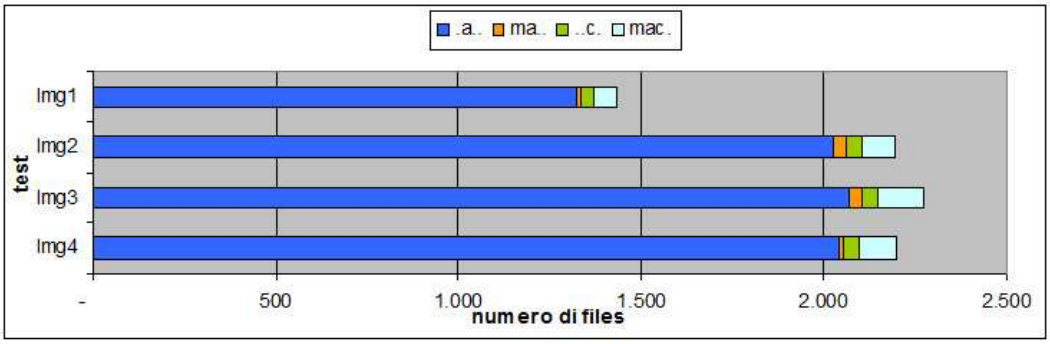



Figura 6.15: Antivirus - macchina accesa per 15 minuti.

Possiamo osservare che, nella Figura 6.15, l'incremento dei files acceduti è ancora una volta notevole. Anche i files mac. registrano degli incrementi, anche se minimi. I files ..c. sono costanti in tutte le immagini analizzate, mentre i files ma.. oscillano, con picchi su Img2 e Img3.

### Apertura e chiusura di un file con Word

Consideriamo il test 35 eseguito su tutte le quattro immagini, ossia *apertura e successiva chiusura di un file con Word*.
Nella Figura 6.16 possiamo osservare che i valori riscontrati su Img2 e Img4 sono abbastanza simili. Leggermente più basso è il numero di files acceduti su Img3 e notevolmente di più quello riscontrato su Img1. Le altre tipologie di modificazioni risultano essere abbastanza costanti.

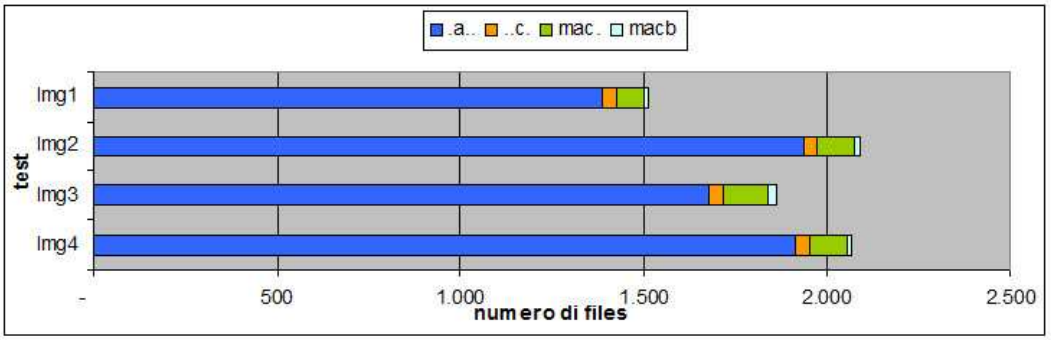



Figura 6.16: Antivirus - apertura e chiusura di un file con Word.

### Collegamento e scollegamento di una penna USB

Consideriamo il test 44 eseguito su tutte le quattro immagini, ossia *collegamento e successivo scollegamento sicuro di una penna USB*.
Contrariamente a quanto ci si sarebbe potuto aspettare, Img4 (scansione antivirus dei dispositivi connessi) non registra particolari ed evidenti differenze rispetto alle altre immagini, ma è anzi abbastanza simile a Img2 e Img3.

L'unica immagine che ovviamente si discosta dalle altre è Img1 che come al solito registra un numero di files acceduti di molto più basso.

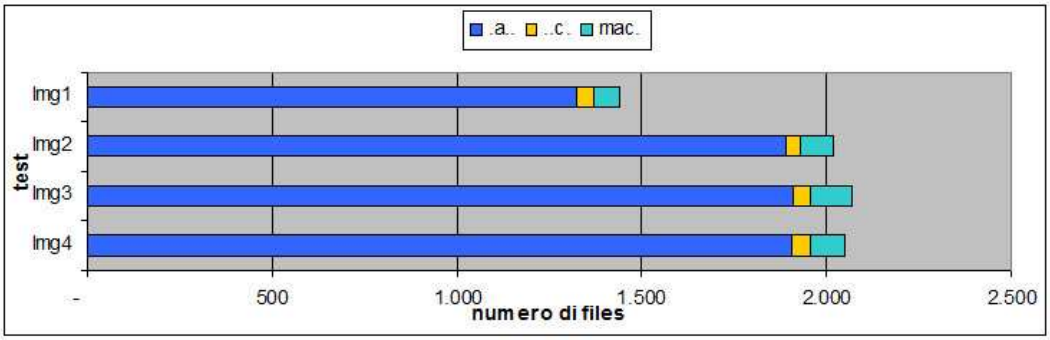



Figura 6.17: Antivirus - collegamento e scollegamento di un drive USB.

### Conclusioni

Avere un software antivirus installato sulla macchina fa registrare un numero di operazioni più elevato rispetto alla stessa macchina priva di protezione. Principalmente queste movimentazioni sono risultate della tipologia accesso. Quando il sistema ha una scansione antivirus pre-impostata all'avvio, non si registrano particolari variazioni. Stesso discorso per le immagini in cui sono impostate diverse modalità di protezione.

# Conclusioni

Questo progetto, ideato per valutare e quantificare le tipologie di alterazioni che avvengono su un'immagine disco quando si verifica un utilizzo improprio della stessa, ha portato alla luce diversi aspetti interessanti.
La delicatezza del reperto informatico è quantomai stata confermata grazie alla presenza di alterazioni in ogni singolo test eseguito. Anche il primo di essi, che rappresenta la minima azione attuata sulla macchina, ossia l'accensione della stessa con spegnimento alla schermata di caricamento, ha fatto registrare delle modificazioni nei file di sistema. Il semplice accesso ad un singolo file, come in questo caso, costituisce a tutti gli effetti un alterazione della macchina, che appare ancora più evidente se si osserva il mutamento del digest della stessa [Pagine 62 e 70].
I successivi test hanno registrato un numero ed una varietà maggiore di modificazioni e rilevato che comunque la tipologia di alterazione che si verifica più frequentemente è l'accesso (a), che rappresenta mediamente il 90% delle operazioni di ogni test. A seguire, in ordine decrescente, le operazioni che registrano più occorrenze sono la modifica dei metadati (c), la modifica del contenuto (m) e per ultimo la creazione ex-novo del file (b). Queste considerazioni sono valide per tutte le copie forensi utilizzate, ma ovviamente avere un software antivirus installato sulla macchina (Img2, Img3 e Img4) genera un numero di modificazioni più elevato, che si percepisce in particolar modo sul numero di files acceduti ed in maniera abbastanza proporzionale sulle restanti operazioni.

Il test che in assoluto ha fatto registrare il maggior numero di operazioni sui file è il 41, *"utilizzando la funzione cerca di Windows, cercare la parola keyword_di_test_1 su tutto il disco C"*, che ha contato ogni volta più 15'000 operazioni. Un risultato notevole se confrontato con gli altri (la soglia dei 2'000 movimenti non è stata altrove superata), ma comunque di facile previsione, dal momento che l'algoritmo di ricerca di Windows accede iterativamente ad ogni file per leggerne il contenuto. Si è dimostrato quindi che utilizzare tale funzione in un contesto reale provocherebbe alterazioni molto ingenti, ben superiori al beneficio che si potrebbe ricavarne.

Come è stato ampiamente discusso, un reperto non andrebbe mai e poi mai utilizzato direttamente; però, nel caso in cui non vi fossero alternative, ed alla luce dei risultati riscontrati, è possibile definire delle linee guida per limitare al minimo le alterazioni.
Come precedentemente accennato, è fortemente sconsigliato ricercare parole tramite la funzione cerca di Windows, l'unica valida alternativa per ottenere tali informazioni è utilizzare software forensi specifici, come ad esempio il già citato Sleuth Kit con Autopsy Forensics Browser.
Per accedere al computer, è fortemente consigliato l'utilizzo di un account con poteri di amministratore che, come visto nel paragrafo 6.3.2, genera un numero inferiore di modificazioni rispetto alla controparte standard. Questa scelta è la più opportuna sia in fase di login, che in quella di vero e proprio utilizzo della macchina.
Nel caso vi fosse necessità di accedere al web, il browser da preferire tra Internet Explorer e Mozilla Firefox è sicuramente (numericamente parlando) il secondo. Il divario tra il numero di operazioni dei due non è eccessivo, ma la natura di queste alterazioni è molto diversa, quindi l'ultima parola deve essere lasciata al computer forenser, che valuti attentamente quale situazione preferire [Figura 6.11].
Parlando invece di suite per l'ufficio, quando è possibile scegliere tra le due alternative Microsoft Office e OpenOffice.org è decisamente da preferirsi la

prima. I test [Figura 6.10] hanno infatti mostrato che così facendo le alterazioni si potrebbero ridurre di quasi 1/3, principalmente in riferimento ai file acceduti.
Molto più numerose sono le considerazioni a cui si potrebbe giungere dalla semplice osservazione dei dati raccolti; si confida nel fatto che questo breve trattato possa contribuire in qualche modo alla diffusione di una metodologia più accurata.

# Bibliografia

## Bibliografia


[AM06] Stefano ATERNO e Paolo MAZZOTTA. *La perizia e la consulenza tecnica. Con approfondimento in tema di Perizie Informatiche*. Cedam, 2006.

[DD07] David D'AGOSTINI e Sabrina D'ANGELO. *Diritto penale dell'informatica: dai computer crimes alla digital forensic*. Experta edizioni, 2007.

[FIN08] Giusella FINOCCHIARO. *Diritto di Internet*. Zanichelli Bologna, 2008.

[FR09] Stefano FRATEEPIETRO e Sandro ROSSETTI. *Deft, manuale d'uso*. Ver. 0.6. 2009.

[GAM] Antonio GAMMAROTA. *Gli aspetti giuridici della prova digitale*.

[GF09] Andrea GHIRARDINI e Gabriele FAGGIOLI. *Computer forensics (Guida completa)*. Apogeo, 2009.

[HAL98] Mark HALLMAN. "Timeline creation and analysis". In: *Sleuthkit and Open Source Digital Forensics Conference*. A cura di Digital Discovery Dallas. 1998.

[HOS98] Chet HOSMER. "Time-Lining Computer Evidence". In: *Information Technology Conference*. A cura di WetStone Technologies Inc. 1998.

[Im05] Tribunale penale di Bologna sezione I monocratica. *Sentenza 21/07/2005 (caso Vierika)*. 2005.

[Ip08] Corte d'appello di Bologna sezione II penale. *Sentenza 30/01/2008 (caso Vierika)*. 2008.

[LZ07] Luca LUPARIA e Giovanni ZICCARDI. *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Giuffrè, 2007.

[MAI04] Cesare MAIOLI. *Dar voce alle prove: elementi di informatica forense.*, 2004.

[MG02] Albert Jr. MARCELLA e Robert S. GREENFIELD. *Cyber Forensics: a eld manual for collecting, examining and preserving evidence of computer crimes*. Auerbach, 2002.

[pen09] Tribunale di Vigevano sezione penale. *Sentenza 31/10/2008 (caso Garlasco)*. 2009.

## Sitografia

[CARti] Brian CARRIER. *Autopsy manual*. Ver. 1.0. Ultima visita: 7 novembre 2011. URL: http://www.sleuthkit.org/autopsy/help/index.html.

[Dftia] Digital-forensics.it. *Computer Forensics analisi dei dati*. Ultima visita: 28 ottobre 2011. URL: http://www.digital-forensics.it/analisi-dei-dati.

[Dftib] Digital-forensics.it. *Computer Forensics catena di custodia*. Ultima visita: 28 ottobre 2011. URL: http://www.digital-forensics.it/catena-di-custodia.

[GROti] Giampietro GROSSELLE. *Accertamenti tecnici ripetibili e non ripetibili*. Ultima visita: 28 ottobre 2011. URL: http://www.crimine.it/pagina.asp?ID=165.

[ILDti] U.S. Department of Justice. Federal Bureau of Investigation. Laboratory Division. *Handbook of forensic*. Ultima visita: 7 novembre 2011. URL: http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf/view.

[Nonti] Nonciclopedia. *Sospensione del servizio*. Ultima visita: 24 ottobre 2011. URL: http://nonciclopedia.wikia.com/wiki/Nonciclopedia:Sospensione_del_servizio.

[Stati] StatCounter. *Global Stats, top 5 browsers from July 2010 to June 2011*. Ultima visita: 22 ottobre 2011. URL: http://gs.statcounter.com/#browser-ww-monthly-201007-201106-bar.

[TPti] Claudio TAMBURRINO (PuntoInformatico.it). *Vasco: Nonciclopedia, ridere di te?* Ultima visita: 24 ottobre 2011. URL: http://punto-informatico.it/3298223/PI/News/vasco-nonciclopedia-ridere-te.aspx.

# Ringraziamenti

Vorrei ringraziare la mia famiglia senza il cui aiuto e sostegno non avrei potuto arrivare a questo traguardo. Riccardo, il mio sostenitore numero uno, i cui occhi color del caffé sono da sempre mia fonte di ispirazione. Tutte le amicizie che sono sopravvissute ai mesi di isolamento sociale necessari al completamento di questo lavoro.

Ringrazio il mio relatore Marco Roccetti, e al mio correlatore Cesare Maioli, entrambi di una disponibilità disarmante. Ultimo ma non ultimo, il dottor Michele Ferrazzano, preziosissimo consigliere nello sviluppo dei capitoli tecnici.